Michelangelo SHDSL

SHDSL VPN Firewall Bridge/ Router

User's Manual Ver. 1.0

digicom

Chapter 1: Introduction

Introduction to your Router

Welcome to the Digicom MICHELANGELO SHDSL Router. Your Digicom SHDSL router is an “all-in-one” unit, combining an SHDSL modem, SHDSL router and Ethernet network switch, providing everything you need to get the machines on your network connected to the Internet over your SHDSL broadband connection. With features such as an SHDSL Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users to the guru requiring advanced features and control over their Internet connection and network.

Features

- **SHDSL Multi-Mode Standard**
  MICHELANGELO SHDSL supports downstream and upstream transmission rates of up to 2.3 / 4.6 Mbps respectively. It also supports rate management that allows SHDSL subscribers to select an Internet access speed suiting their needs and budgets. It follows ITU standard PAM16 Line Code complies with G.991.2 and G.994.1 standards. Furthermore it can support Annex A and B operating mode.

- **Fast Ethernet Switch**
  A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.

- **Multi-Protocol to establish a connection**
  It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

- **Quick Installation Wizard**
  It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf the Internet immediately.

- **Universal Plug and Play (UPnP) and UPnP NAT Traversal**
  This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

- **Network Address Translation (NAT)**
  Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

- **SOHO Firewall Security with DoS and SPI**
  Along with the built-in NAT natural firewall feature, the router also provides advanced hacker pattern-filtering protection. It can automatically detect and block Denial of Service (DoS) attacks. The router is built with Stateful Packet Inspection (SPI) to determine if a data packet is allowed through the firewall to the private LAN.

- **Domain Name System (DNS) relay**
  It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router’s IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

- **Dynamic Domain Name System (DDNS)**
  The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.

- **Quality of Service (QoS)** QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router ay lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

- **Virtual Private Network (VPN)**
  It allows user to make a tunnel with a remote site directly to secure the data transmission among the connection. User can use embedded PPTP and L2TP client/server, IKE and IPSec which are supported by this router to make a VPN connection or users can run the PPTP client in PC and the router already provides IPSec and PPTP pass through function to establish a VPN connection if the user likes to run the PPTP client in his local computer.

- **Virtual Server ("port forwarding")**
  Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

- **Rich Packet Filtering**
  Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.

- **Dynamic Host Configuration Protocol (DHCP) client and server**
  In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

- **Static and RIP1/2 Routing**
  It has routing capability and supports easy static routing table or RIP1/2 routing protocol.

- **Simple Network Management Protocol (SNMP)**
  It is an easy way to remotely manage the router via SNMP.

- **Web based GUI**
  It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

- **Firmware Upgradable**
  Device can be upgraded to the latest firmware through the WEB based GUI.

- **Rich Management Interfaces**
  It supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

Chapter 2: Installing the Router

Important note for using this router

Warning

- ✓ **Do not use this router in high humidity or high temperatures.**
- ✓ **Do not use the same power source for this router as other equipment.**
- ✓ **Do not open or repair the case yourself. If this router is too hot, turn off the power immediately and have it repaired at a qualified service center.**
- ✓ **Avoid using this product and all accessories outdoors.**

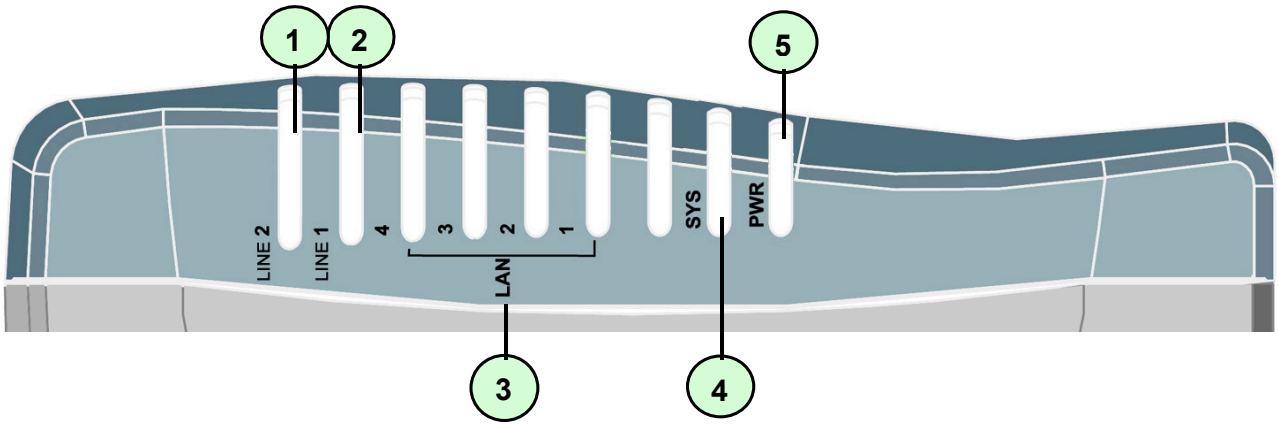
Attention

- ✓ **Place this router on a stable surface.**
- ✓ **Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage this router.**

Package Contents

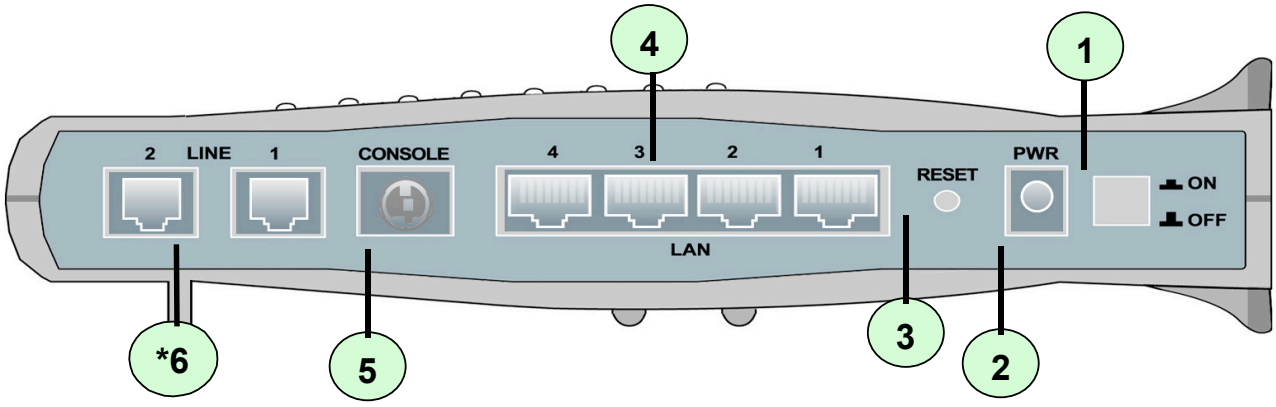
- SHDSL Router
- CD-ROM containing the online manual
- RJ-11 SHDSL / telephone Cable
- Ethernet (CAT-5 LAN) Cable
- Console (PS2-RS232) Cable
- AC-DC power adapter (12V DC, 1A)
- Quick Start Guide

The Front LEDs of MICHLANGELO SHDSL



LED		Meaning
1 2	**LINE 1 & 2**	Lit when successfully connected to SHDSL line and it is synchronized.
3	**LAN Port** **1 X — 4 X** **(RJ-45 connector)**	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps. Blinking when data is Transmitted / Received.
4	**SYS**	Lit when the system is ready.
5	**PWR**	Lit when power is ON.

The Rear Ports of MICHELANGELO SHDSL



NOTE: *Michelangelo SHDSL has two Line jack ports.*

Port		Meaning
1	**Power Switch**	Power ON/OFF switch
2	**PWR**	Connect the supplied power adapter to this jack.
3	**RESET**	To be sure the device is being turned on → press RESET button for: **1-3 seconds**: quick reset the device. **6 seconds above, and power off, power on the device**: restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). **Caution**: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.
4	**LAN** **1X — 4X (RJ-45 connector)**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
5	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
6	**LINE** **1X — 2X (RJ-11 connector**	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to SHDSL line.

Cabling

One of the most common causes of problems is bad cabling or SHDSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and SHDSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Chapter 3: Basic Installation

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect with the router, either through an external repeater hub to the router or directly connecting with PCs. However, to be sure PCs have an Ethernet interface installed properly prior to connecting to the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation.

Any TCP/IP capable workstation can be used to communicate with or through the router. To configure other types of workstations, please consult the manufacturer's documentation.

Connecting Your Router

1. Connect the Router to a **LAN** (Local Area Network) and the SHDSL **LINE**.
2. Power on the device.
3. Make sure the **PWR** and **SYS** LEDs are lit steadily and that the relevant **LAN and LINE** LED are lit.

Configuring PCs in Windows in Window XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click **Network Connections**.
2. Double-click **Local Area Connection**. **(See Figure 3.1)**

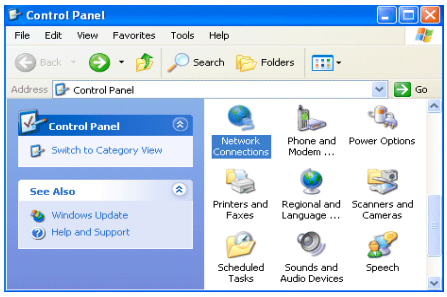


Figure 3.1: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. (**See Figure 3.2)**

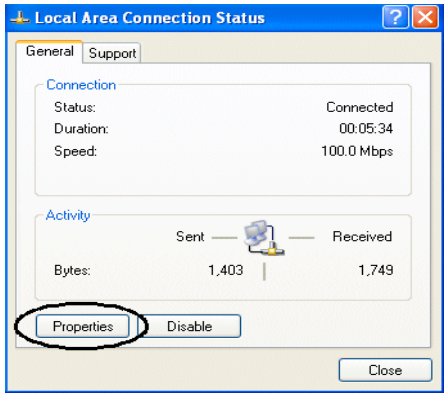


Figure 3.2: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. (**See Figure 3.3)**

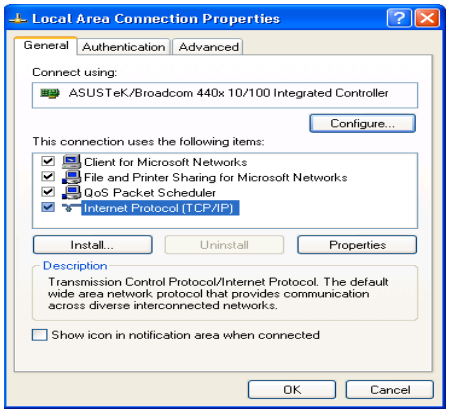

Local Area Connection Properties
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

Figure 3.3: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (**See Figure 3.4**)
6. Click **OK** to finish the configuration.

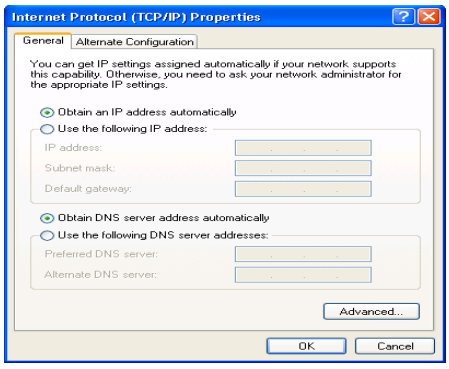

Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

Figure 3.4: IP Address & DNS Configuration

Configuring PCs in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network and Dial-up Connections**.
2. Double-click **Local Area ("LAN") Connection**. **(See Figure 3.5)**

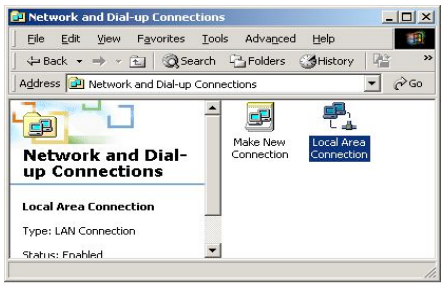


Figure 3.5: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. **(See Figure 3.6)**

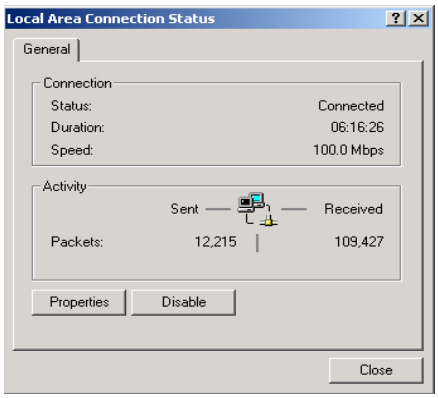


Figure 3.6: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. **(See Figure 3.7)**

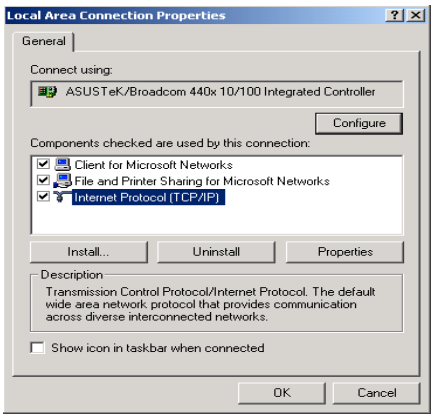


Figure 3.7: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. **(See Figure 3.8)**
6. Click **OK** to finish the configuration.

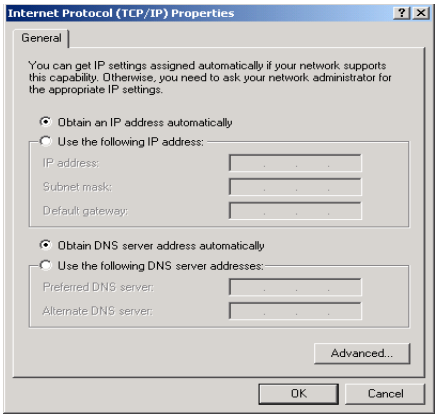

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3.8: IP Address & DNS Configuration

Configuring PC in Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC. (**See Figure 3.9)**
3. Click **Properties**.

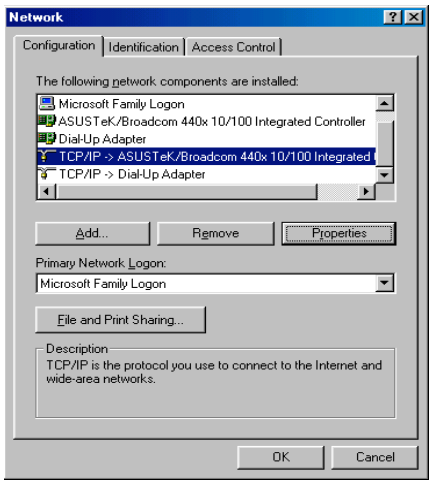


Figure 3.9: TCP / IP

4. Select the **IP Address** tab. In this page, click the Obtain an IP address automatically radio button. (**See Figure 3.10)**

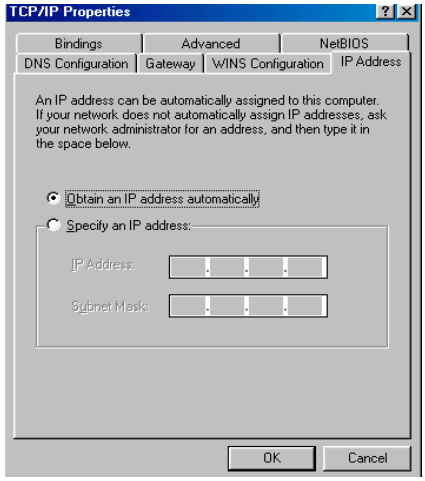

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Figure 3.10: IP Address

5. Then select the **DNS Configuration** tab. **(See Figure 3.11)**
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

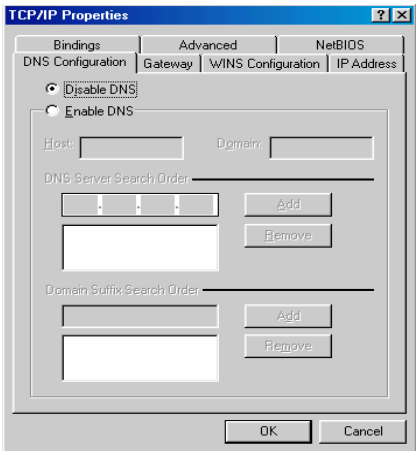


Figure 3.11: DNS Configuration

Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**. (**See Figure 3.12)**

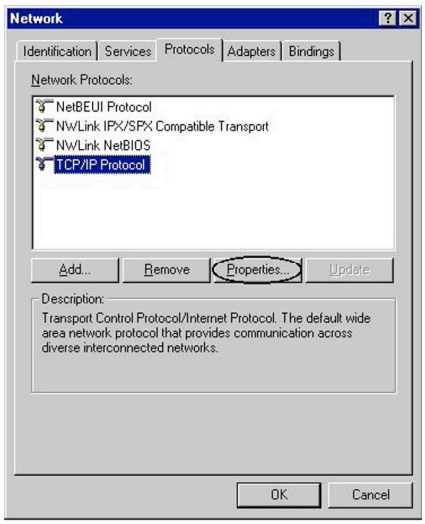


Figure 3.12: TCP / IP

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**. (**See Figure 3.13)**

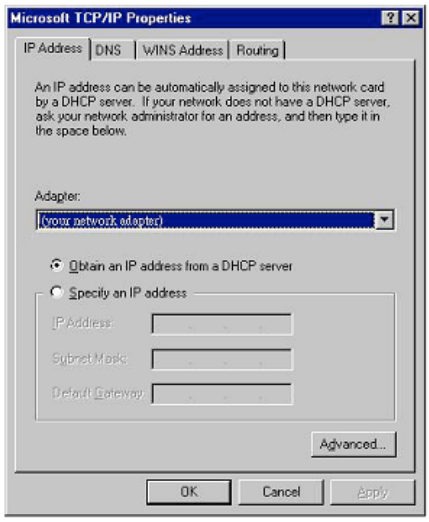

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Figure 3.13: IP Address

Factory Default Settings

Before configuring your, you need to know the following default settings.

Web Interface (Username and Password)

- Username: admin
- Password: admin

The default username and password are “**admin**” and “**admin**” respectively.

Attention

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.

Device LAN IP settings:

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site:

- PPPoE

DHCP server

- DHCP server is enabled.
- Start IP Address: 192.168.1.100
- IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) and PPPoE.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually).
PPPoE / PPPoE with Pass-through	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually). In addition, additional WAN address can be assigned using PPPoE dialer.
PPPoA	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually).
RFC 1483 Bridged	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.
RFC 1483 Routed	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA Routed (IP over ATM)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click "**Go**", a user name and password window prompt will appear. **The default username and password are "admin" and "admin"** respectively**. (See Figure 3.14)**

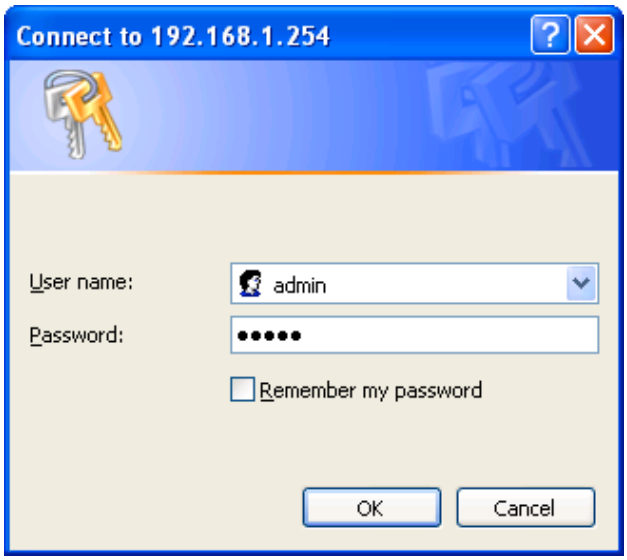


Figure 3.14: User name & Password Prompt Window

Congratulation! You are now successfully logon to the SHDSL Router!

Chapter 4: Configuration

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status**
  - ARP Table
  - Routing Table
  - DHCP Table
  - PPTP Status
  - IPSec Status
  - L2TP Status
  - Email Status
  - Event Log
  - Error Log
  - NAT Sessions
  - Diagnostic
  - UPnP Portmap
- **Quick Start**
- **Configuration**
  - LAN
  - WAN
  - System
  - Firewall
  - VPN
  - QoS
  - Virtual Server
  - Time Schedule
  - Advanced
- **Save Config to FLASH**
- **Language** (provides user interface in English and French languages).
- **Logout**

Please click the links to see the relevant sections of this manual for detailed instructions on how to configure the SHDSL VPN Firewall Bridged Router.

Status

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.

ARP Table

IP <> MAC List

IP Address	MAC Address	Interface	Static
192.168.1.187	00:0c:6e:bd:11:6d	iplan	no

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

MAC Address: The MAC (Media Access Control) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

- "**no**" for dynamically-generated ARP table entries
- "**yes**" for static ARP table entries added by the user

Routing Table

Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost
✓	0.0.0.0	0.0.0.0	192.168.21.1	1

RIP Routing Table

Destination	Netmask	Gateway	Cost

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway/Interface: The IP address of the gateway or existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table

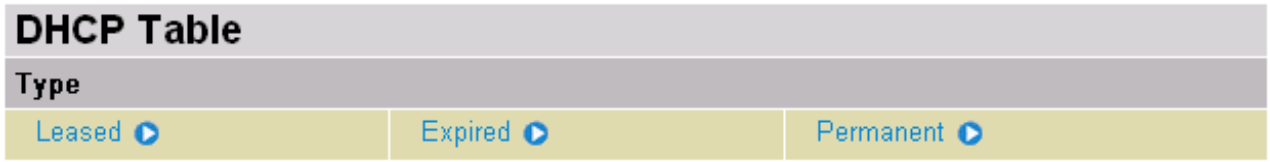
Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway: The IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

DHCP Table



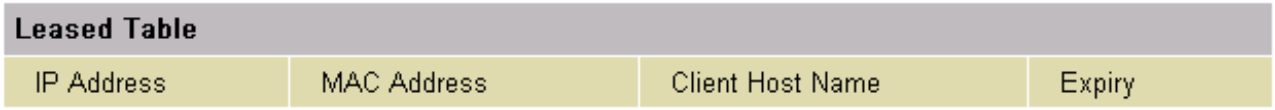
Leased: The DHCP assigned IP addresses information.

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

Leased Table



IP Address: The IP address that assigned to client.

MAC Address: The MAC address of client.

Client Host Name: The Host Name (Computer Name) of client.

Expiry: The current lease time of client.

Expired Table

Please refer the **Leased Table**.

Permanent Table

Name: The name you assigned to the Permanent configuration.

IP Address: The fixed IP address for the specify client.

MAC Address: The MAC Address that you want to assign the fixed IP address

Maximum Lease Time: The maximum lease time interval you allow to clients.

PPTP Status

This shows details of your configured PPTP VPN Connections.

PPTP Status

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/PPTP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular PPTP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

Tunnel Connected: Whether the VPN Tunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

IPSec Status

This shows details of your configured IPSec VPN Connections.

IPSec Status

VPN Tunnels

Name	Active	Connection State	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA

Name: The name you assigned to the particular VPN entry.

Active: Whether the VPN Connection is currently Active.

Connection State: Whether the VPN is Connected or Disconnected.

Statistics: Statistics for this VPN Connection.

Local Subnet: The local IP Address or Subnet used.

Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

L2TP Status

This shows details of your configured L2TP VPN Connections.

L2TP Status

VPN/L2TP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/L2TP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular L2TP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

Tunnel Connected: Whether the VPN Tunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

Email Status

Details and status for the Email Account you have configured the router to check. Please see the **Advanced** section of this manual for details on this function.

Email Status

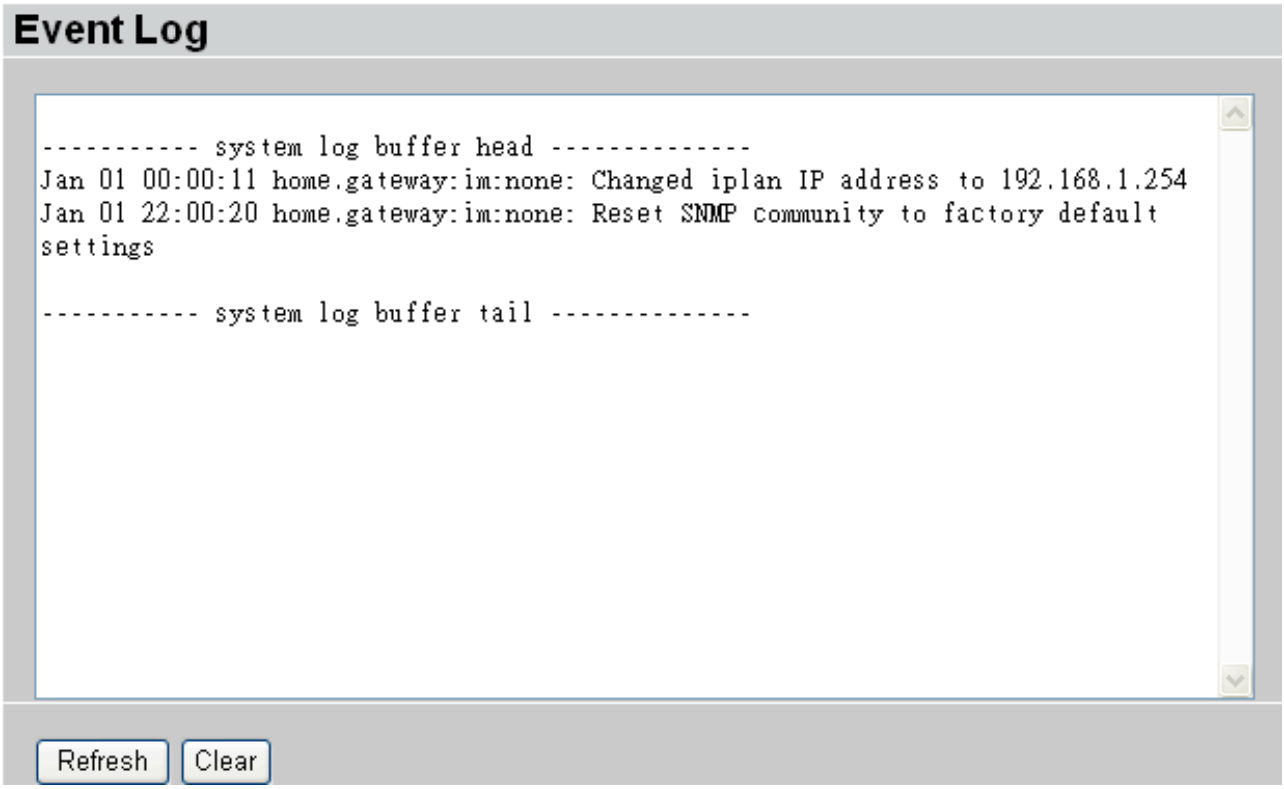
Email Account

Account Name	username
POP3 Mail Server	pop3.mail.com
Email Status	No mail

Reset Status | Check Now

Event Log

This page displays the router's Event Log entries. Major events are logged to this window, such as when the router's SHDSL connection is disconnected, as well as Firewall events when you have enabled Intrusion or Blocking Logging in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.

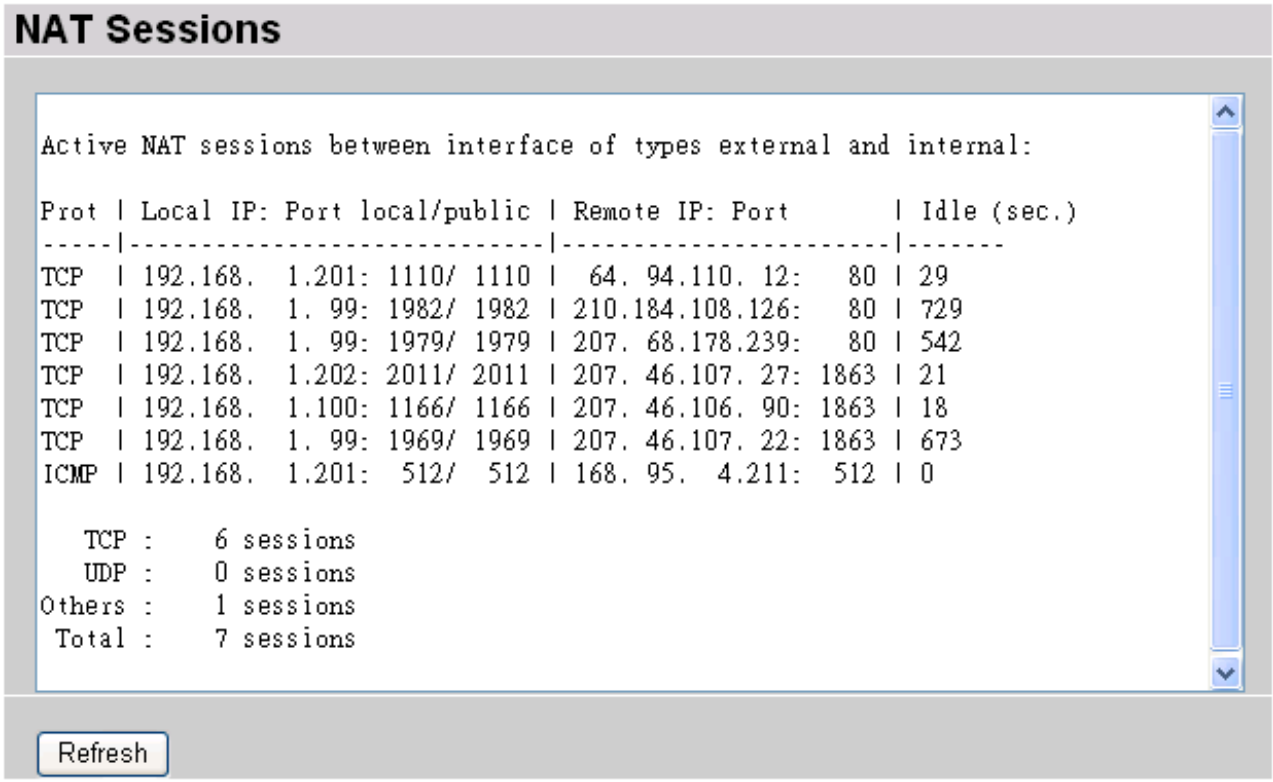

Event Log
---------- system log buffer head --------------
Jan 01 00:00:11 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 01 22:00:20 home.gateway:im:none: Reset SNMP community to factory default settings
---------- system log buffer tail --------------
Refresh
Clear

Error Log

Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.

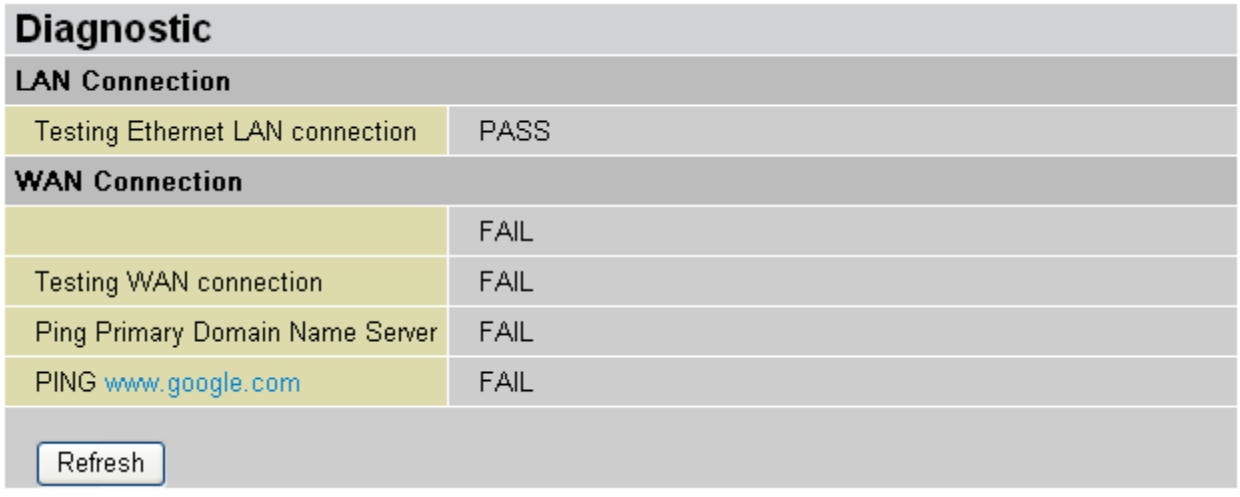
NAT Sessions

This section lists all current NAT sessions between interface of types external (WAN) and internal (LAN).



Diagnostic

It tests the connection to computer(s) which is connected to LAN ports and also the WAN Internet connection. If **PING www.google.com** is shown FAIL and the rest is P ASS, you ought to check your PC's DNS settings is set correctly.



UPnP Portmap

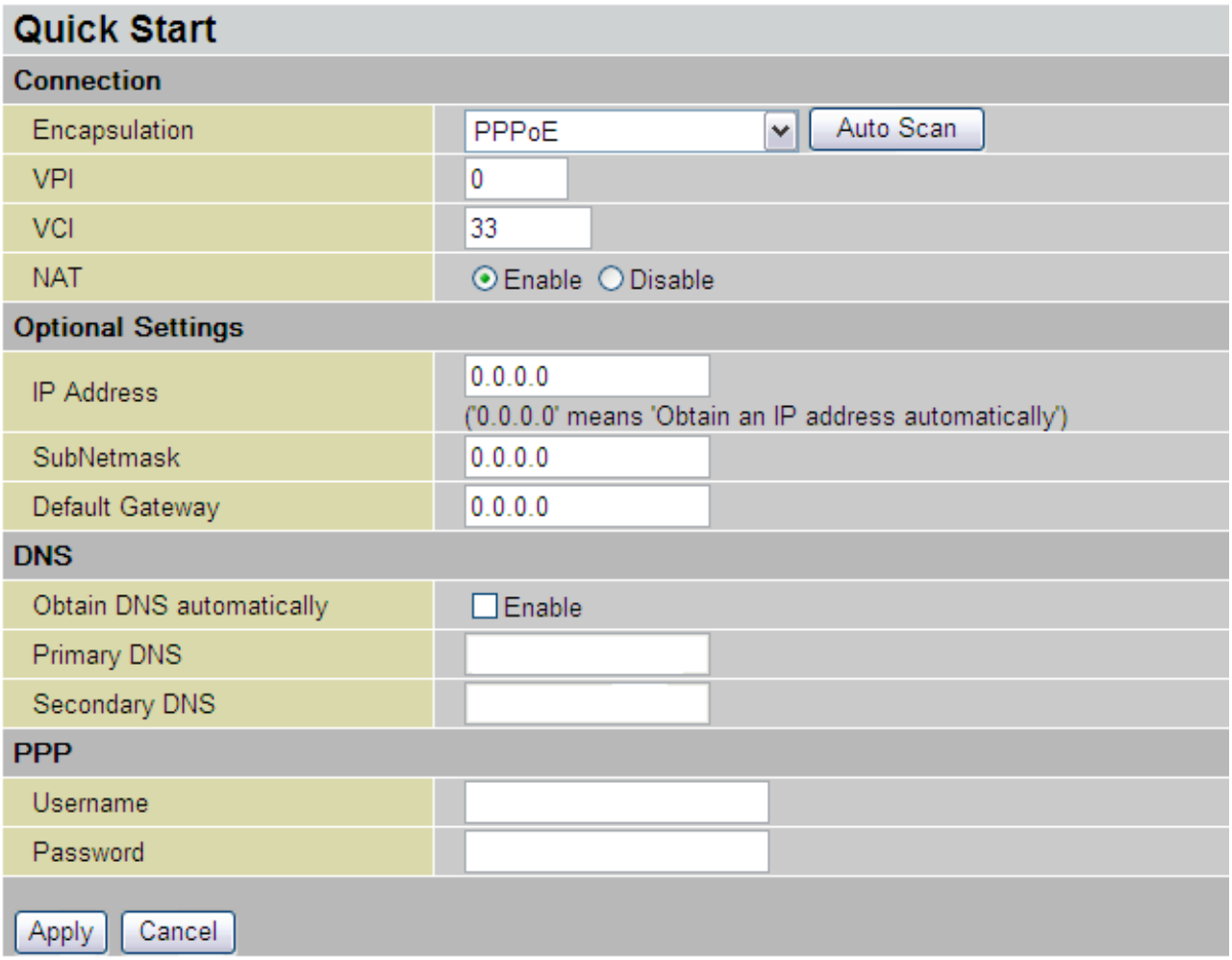
The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the **Advanced** section of this manual for more details on UPnP and the router's UPnP configuration options.

UPnP Portmap

UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address
emwebigd1024	udp	35324 ~ 35324	15852 ~ 15852	192.168.1.205
emwebigd1025	tcp	48888 ~ 48888	14811 ~ 14811	192.168.1.205
emwebigd1063	udp	9210 ~ 9210	15169 ~ 15169	192.168.1.202
emwebigd1064	tcp	50937 ~ 50937	14500 ~ 14500	192.168.1.202

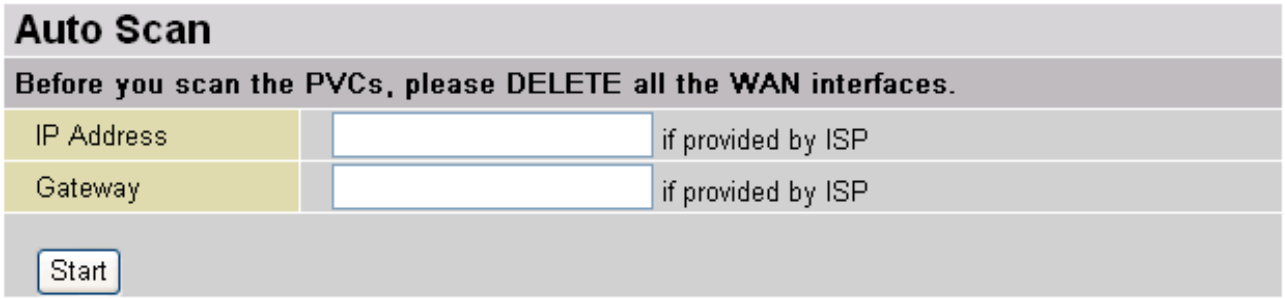
Quick Start



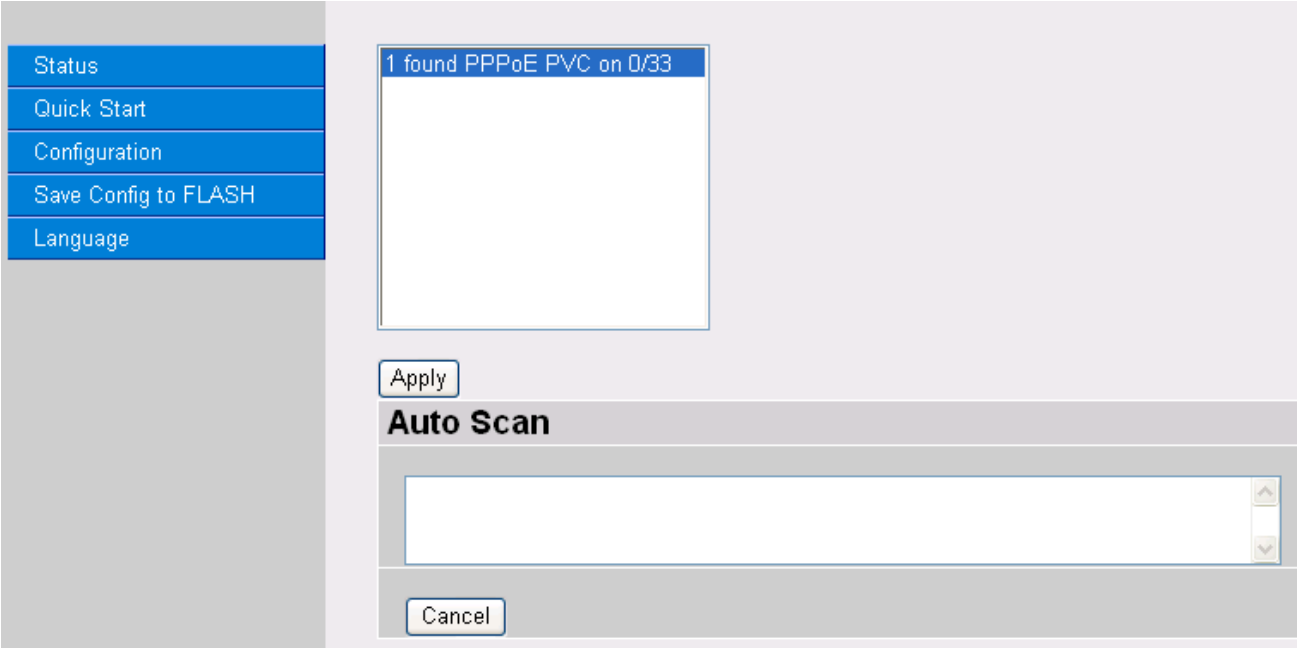
For detailed instructions on configuring your WAN settings, please see the **WAN** section of this manual.

Usually, the only details you will need for the Quick Start wizard to get you online are your login (often in the form of *username@ispname*), your password and the encapsulation type. In additional, you have the option to provide specific DNS as your desire, or check the **Enable** box to get the DNS automatically from your ISP.

Your ISP will be able to supply all the details you need, alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to attempt to determine the Encapsulation types offered by your ISP.



Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful you will then be presented with a list of supported options:



Select the desired option from the list and click **Apply** to return to the Quick Start interface to continue configuring your ISP connection. Please note that the contents of this list will vary, depending on what is supported by your ISP.

Configuration

When you click this item, you get following sub-items to configure your router.

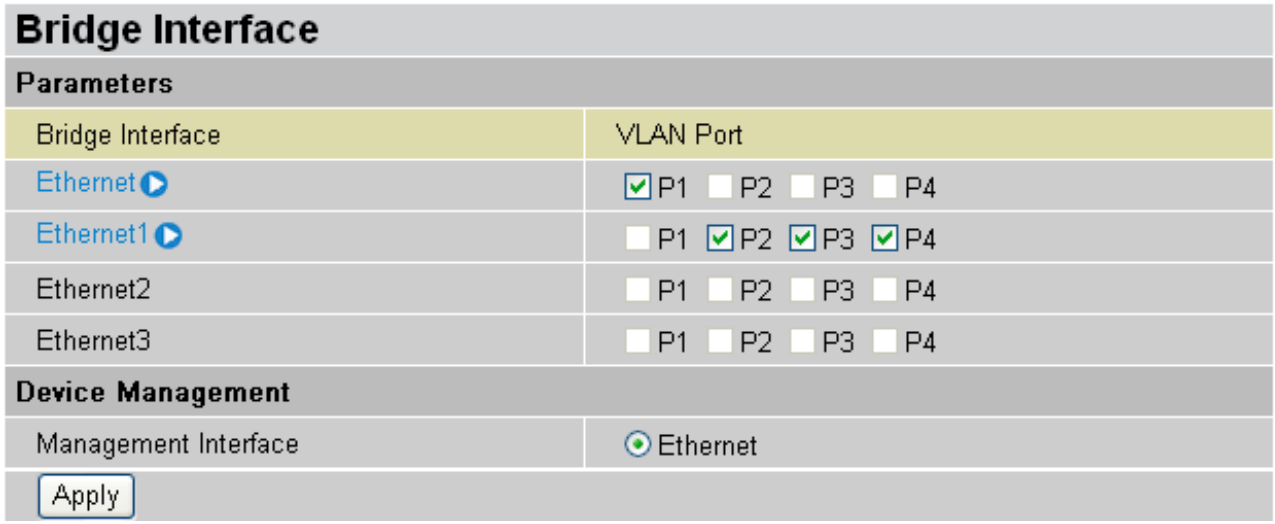
LAN, WAN, System, Firewall, VPN, QoS, Virtual Server, Time Schedule and **Advanced**

These functions are described below in the following sections.

LAN (Local Area Network)

Here are the items within LAN section: **Bridge Interface, Ethernet, IP Alias, Ethernet Client Filter, Port Settings** and **DHCP Server**.

Bridge Interface



You can setup member ports for each VLAN group under Bridge Interface section. From the example, two VLAN groups need to be created.

Ethernet: P1 (Port 1)

Ethernet1: P2, P3 and P4 (Port 2, 3, 4). Uncheck P2, P3, P4 from Ethernet VLAN port first.

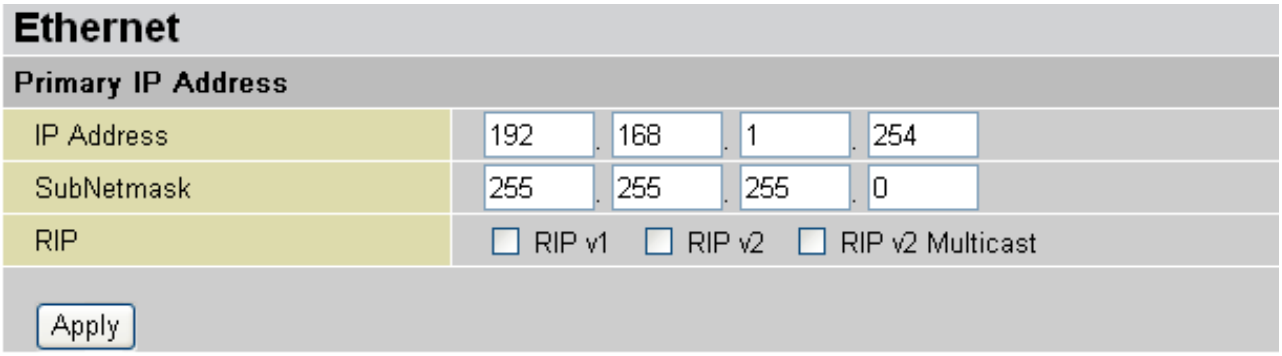
Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4

Management Interface: To specify which VLAN group has possibility to do device management, like doing web management.

Note: NAT/NAPT can be applied to management interface only.

Ethernet



Primary IP Address

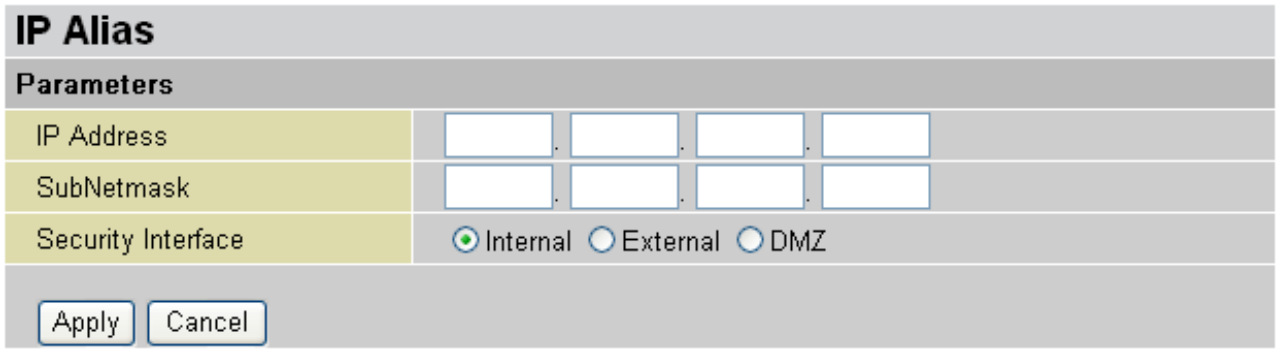
IP Address: The default IP on this router.

SubNetmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

IP Alias

This function supports to create multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



IP Address: Specify an IP address on this virtual interface.

SubNetmask: Specify a subnet mask on this virtual interface.

Security Interface: Specify the firewall setting on this virtual interface.

Internal: The network is behind NAT. All traffic will do network address translation when sending out to Internet if NAT is enabled.

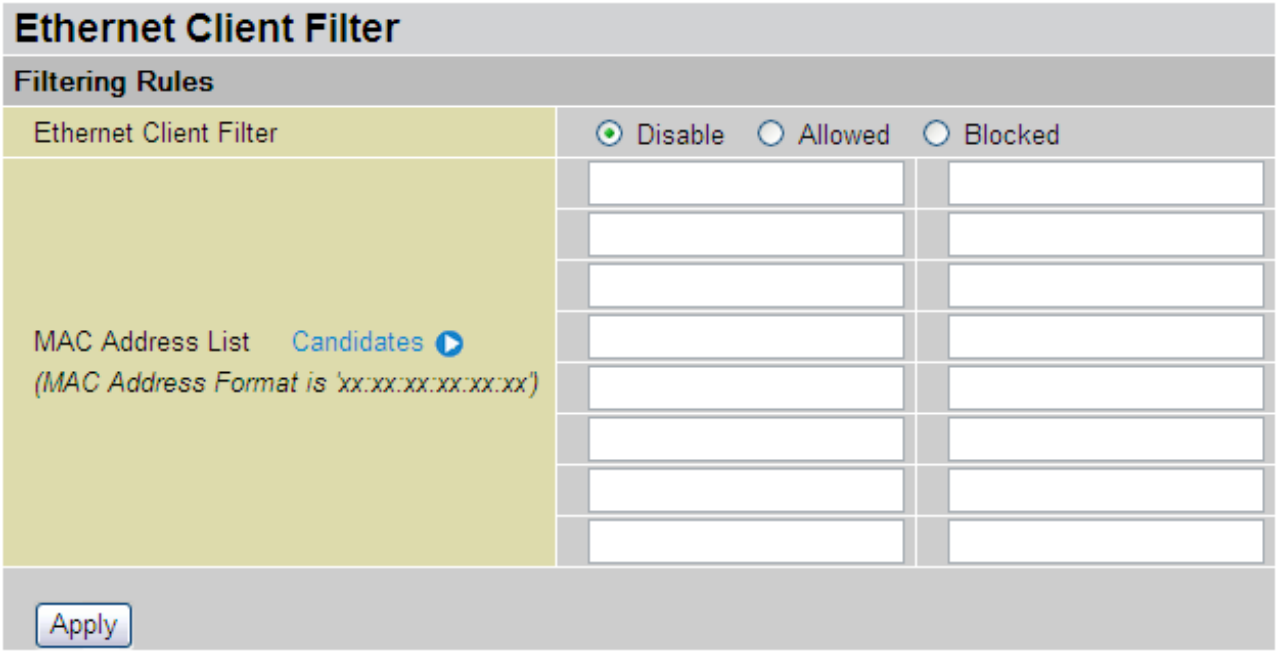
External: There is no NAT on this IP interface and connected to the Internet directly. Mostly it will be used when providing multiple public IP addresses by ISP. In this case, you can use public IP address in local network which gateway IP address point to the IP address on this interface.

DMZ: Specify this network to DMZ area. There is no NAT on this interface.

Ethernet Client Filter

The Ethernet Client Filter supports up to 16 Ethernet network machines that helps you to manage your network control to accept traffic from specific authorized machines or can restrict unwanted machine(s) to access your LAN.

There are no pre-define Ethernet MAC address filter rules; you can add the filter rules to meet your requirements.



Ethernet Client Filter: Default setting is set to **Disable**.

⊙ **Allowed:** check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click Candidates. Make sure your PC's MAC is listed.

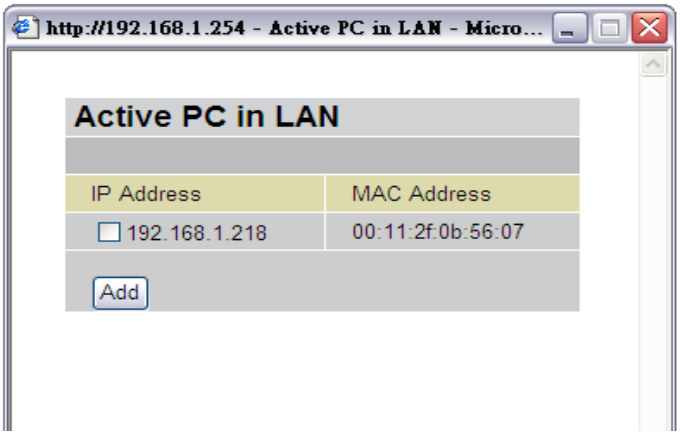
⊙ **Blocked:** check to prevent unwanted device accessing your LAN by insert the MAC Address in the space provided or click Candidates. Make sure your PC's MAC is not listed.

The maximum client is 16. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number **0** - **9** and letters **a** - **f** are acceptable.

Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.

Candidates: automatically detects devices connected to the router through the Ethernet. .

Candidates **_ Active PC in LAN**

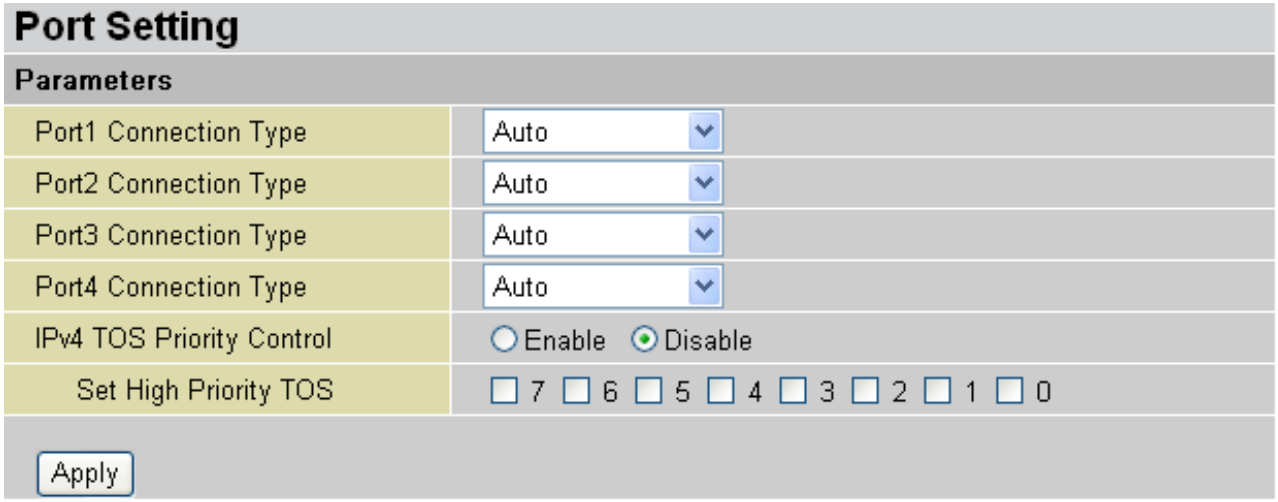


Active PC in LAN displays a list of individual Ethernet device's IP Address & MAC Address which connecting to the router.

You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table. The maximum Ethernet client is 16.

Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



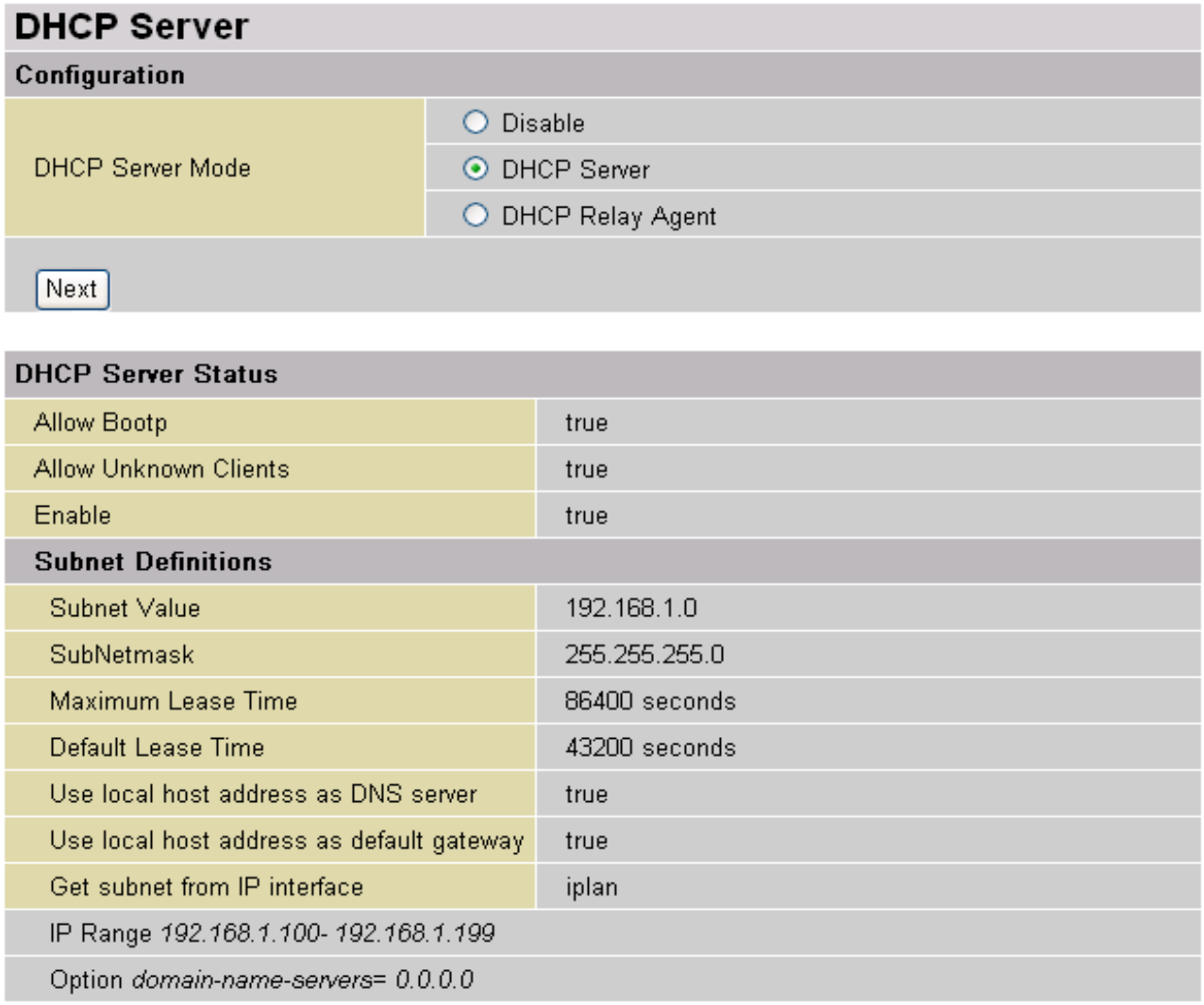
Port # Connection Type: Six options to choose from: Auto, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The default is **Auto**, which users should keep unless there are specific problems with PCs not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

This feature uses bits 0-5 to classify the packet's priority. If the packet is high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the TOS field matches the checked values in the table (0 to 63), this packet will be treated as high priority.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.



To disable the router's DHCP Server, check **Disabled** and click **Next,** then click **Apply.** When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PCs on your network, and set the default gateway for each PCs to the IP address of the router (by default this is 192.168.1.254).

To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network).

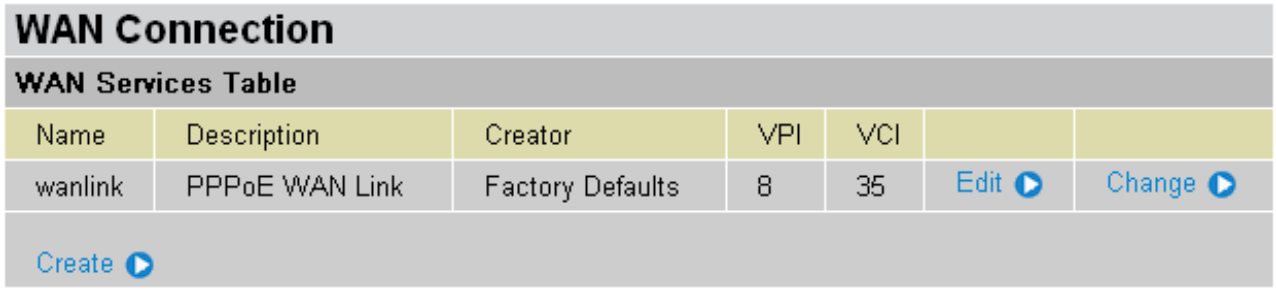
If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

Click **Apply** to enable this function.

WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and the Internet. Here are the items within the **WAN** section: **ISP**, **DNS** and **SHDSL**.

ISP



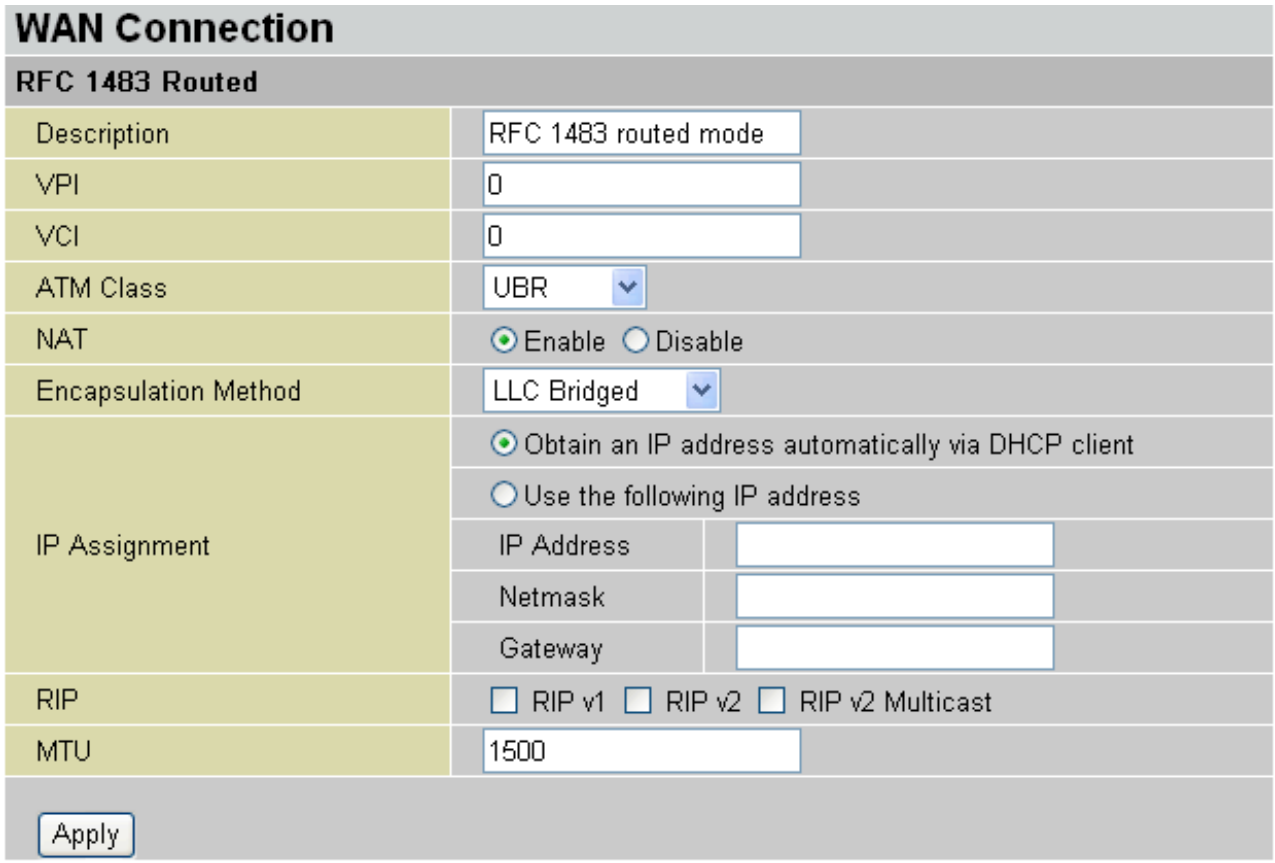
The factory default is PPPoE. If your ISP uses this access protocol, click **Edit** to input other parameters as below. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

Some of ISP may provide more service via different WAN connection. In case, you can create more connections by clicking **Create**. The device can support maximum up to 8 WAN connections.

Note: The application of multiple WAN connections is depend on your Service Provider.

A simpler alternative is to select **Quick Start** from the main menu on the left. Please see the Quick Start section of the manual for more information.

RFC 1483 Routed Connections



Description: User-definable name for the connection.

VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Encapsulation method: Selects the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP.

IP Assignment

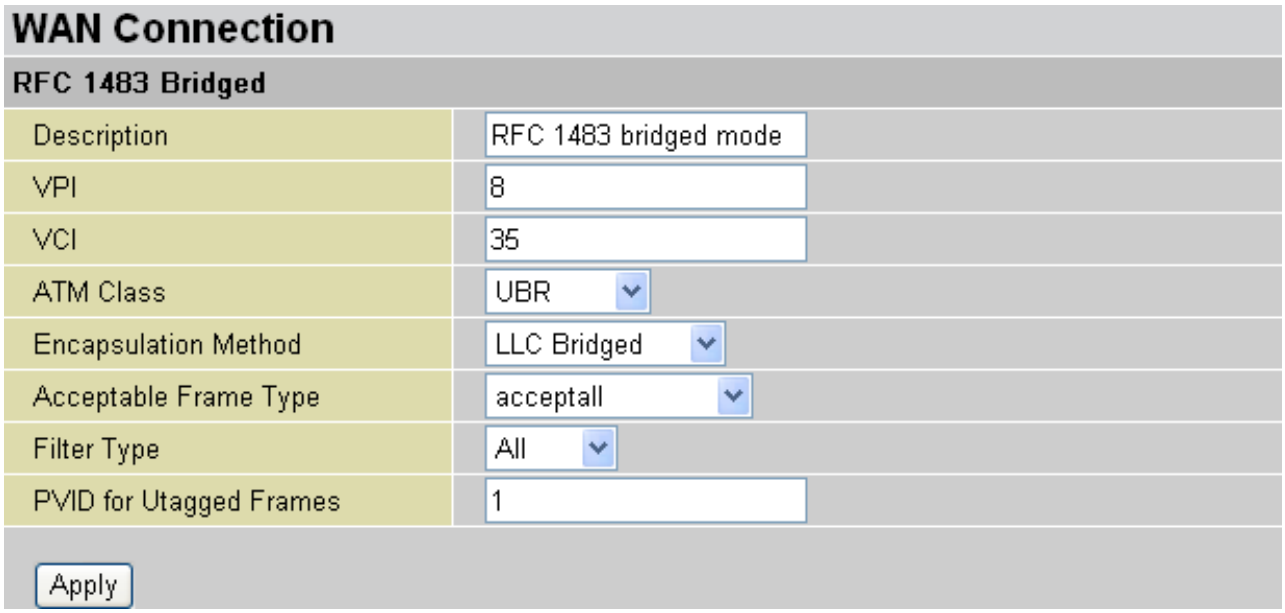
⊙ **Obtain an IP address automatically via DHCP client:** specify if the Router can get an IP address from the ISP (Internet Service Provider) automatically.

⊙ **Use the following IP Address:** Specify the IP address manually; the IP should be given by you our ISP.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RFC 1483 Bridged Connections



Description: User-definable name for the connection.

VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

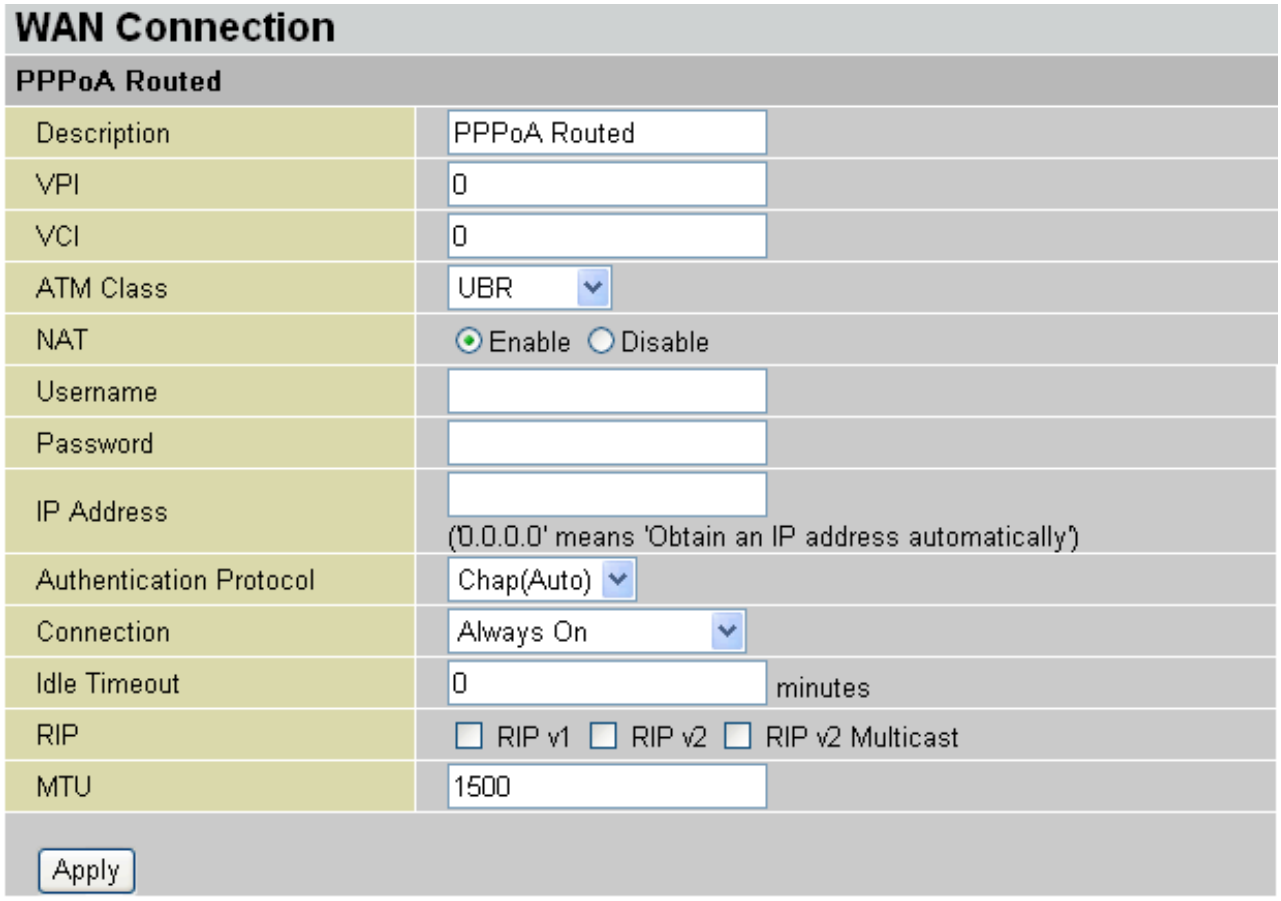
Acceptable Frame Type: Specify what kind of traffic can through this connection, all traffic or only VLAN tagged.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

PVID for Untagged Frames: PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID. The valid value range for PVID is 1~4094.

PPPoA Routed Connections



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

IP Address: Specify an IP address allowed to logon and access the router's web server..

Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.

Authentication Protocol Type: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

- **Always on:** If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
- **Connect on Demand:** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

- **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoA)

LLC Header: Selects encapsulation mode, true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can equest a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

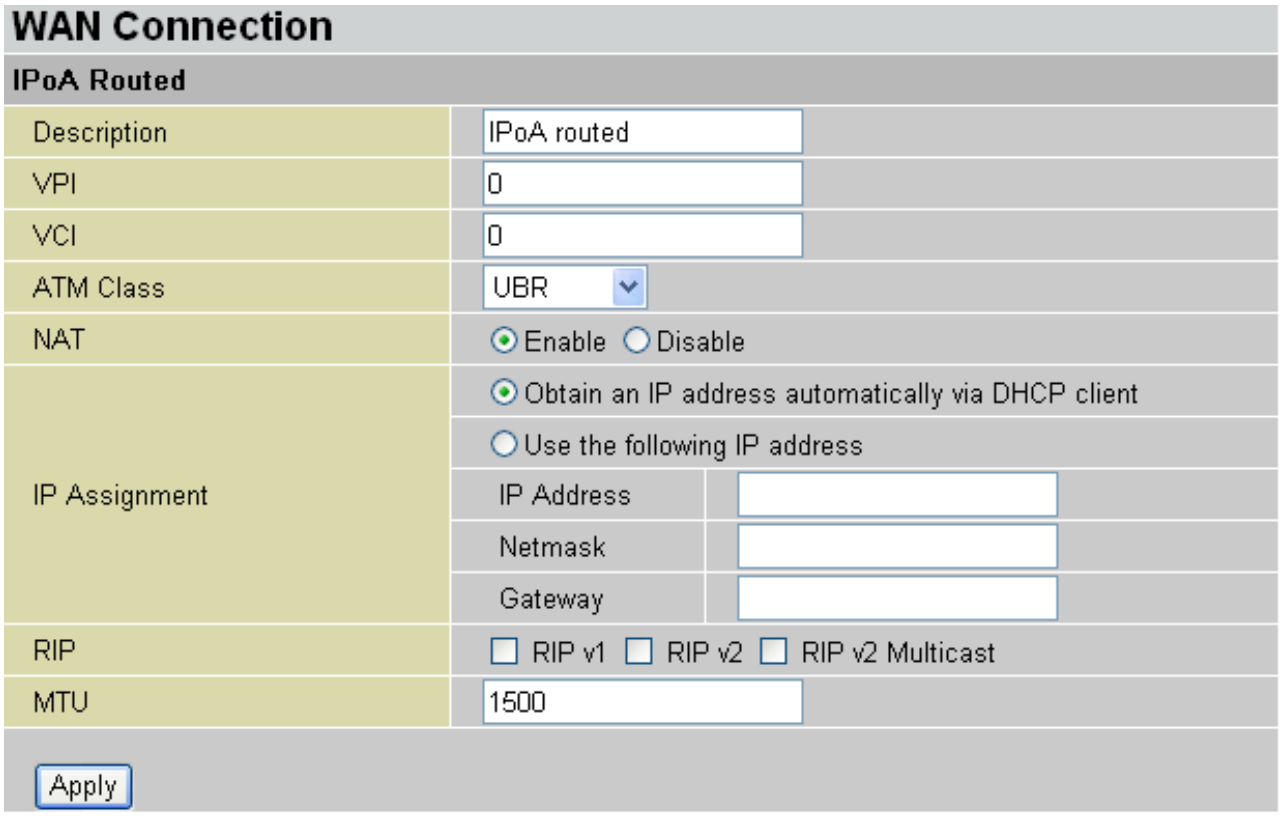
Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

IPoA Routed Connections



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Assignment

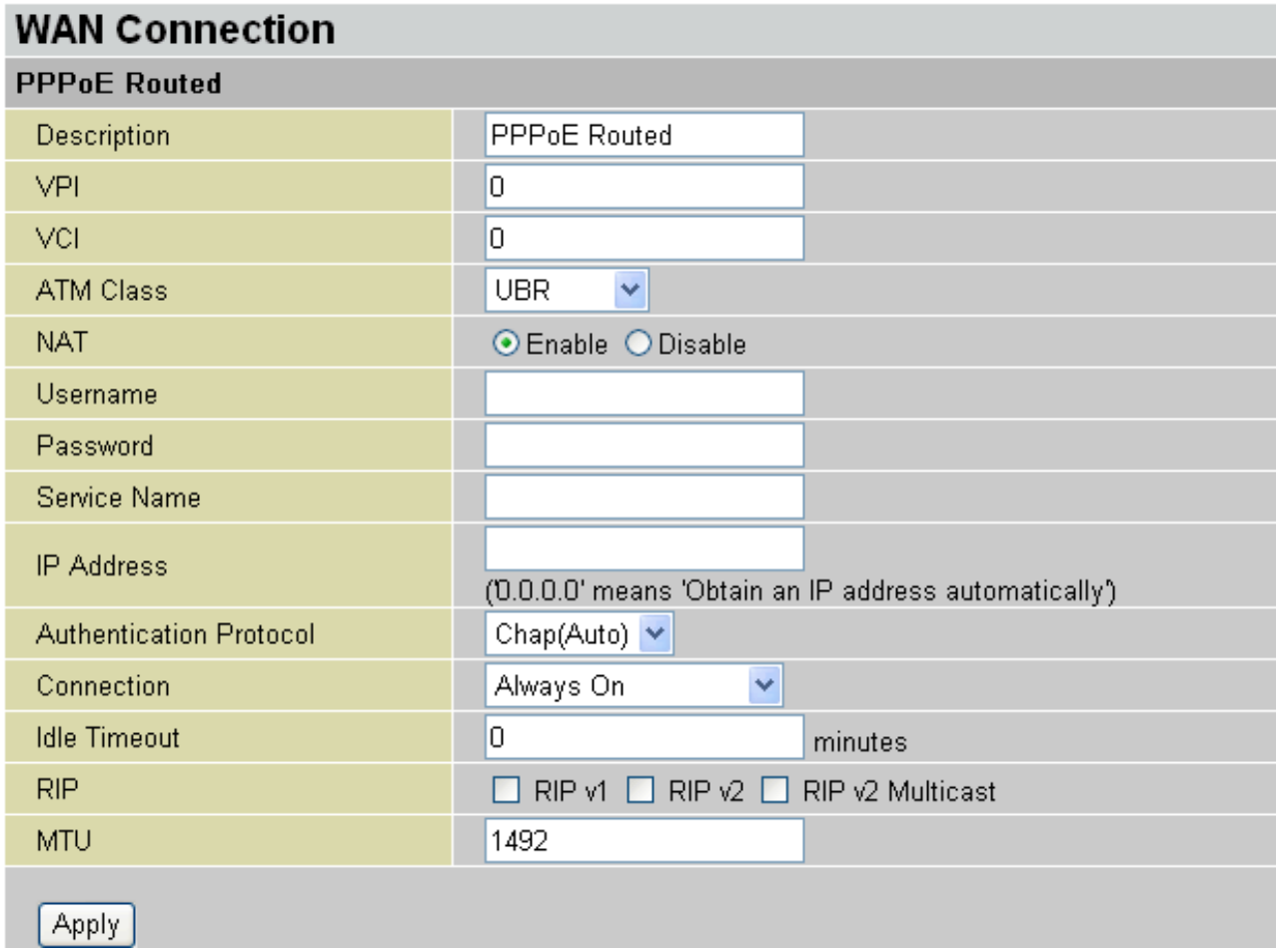
⊙ **Obtain an IP address automatically via DHCP client:** specify if the Router can get an IP address from the ISP (Internet Service Provider) automatically.

⊙ **Use the following IP Address:** Specify the IP address manually; the IP should be given by you our ISP.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE Connections



Description: User-definable name for this connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

Authentication Protocol: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.

Connection

- **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- **Connect on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

⊙ **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoE)

LLC Header: Selects encapsulation mode, true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

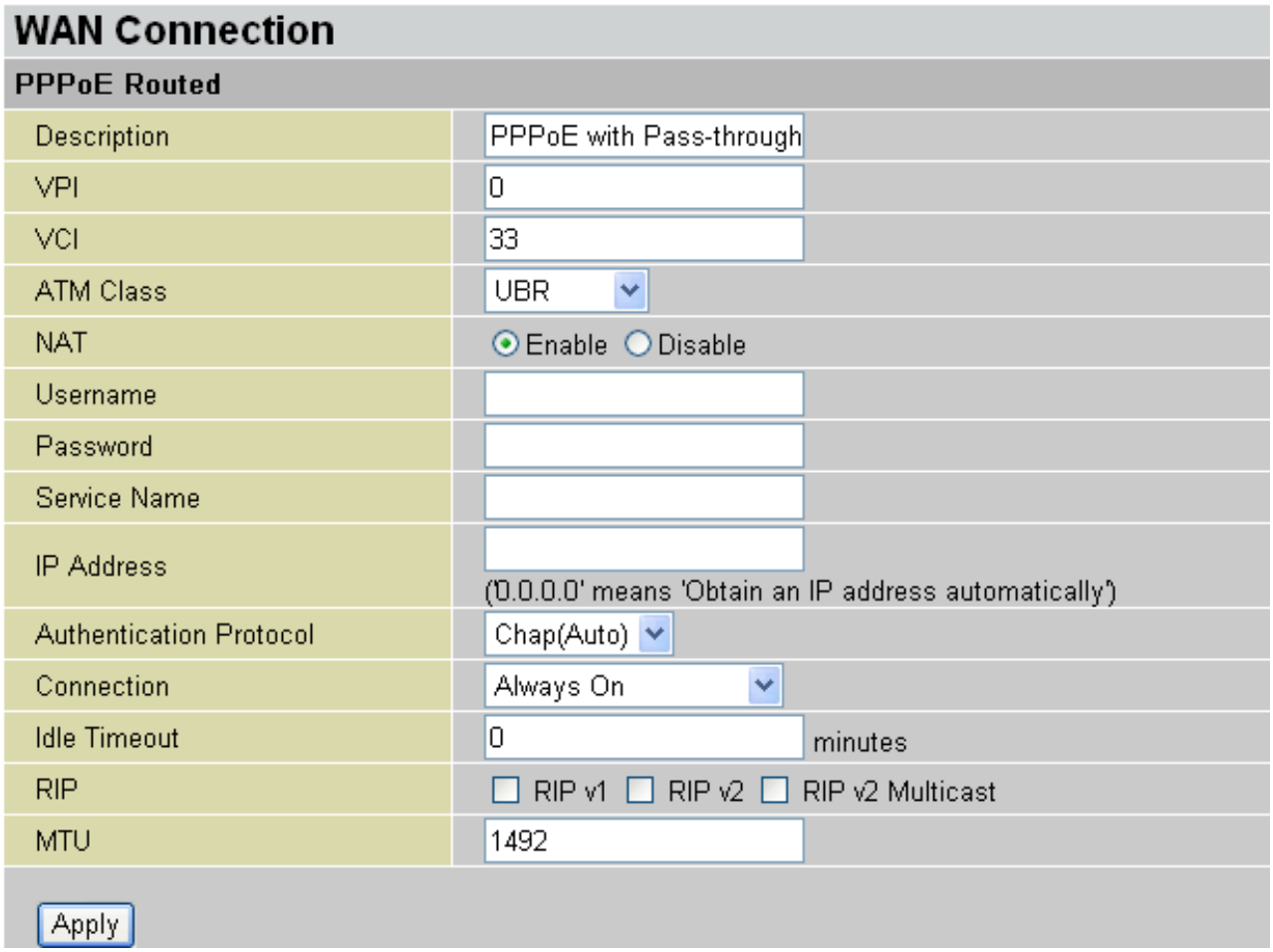
Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

PPPoE with Pass-through Connections

PPPoE with pass-through adapts the following method: PPPoE Routed mode + 1483 Bridge Mode. With pure PPPoE connection, the router can get one WAN address to the router. With the PPPoE and PPPoE pass-through, concurrently, it allows user to have a WAN address assigned to the router but also able to get another WAN IP from ISP using PPPoE dialer (e.g WinPoETor Windows XP PPPoE Dialer) at the same time.



Description: User-definable name for this connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

Authentication Protocol: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

- **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

⊙ **Connect on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

⊙ **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoE)

LLC Header: Selects encapsulation mode, true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

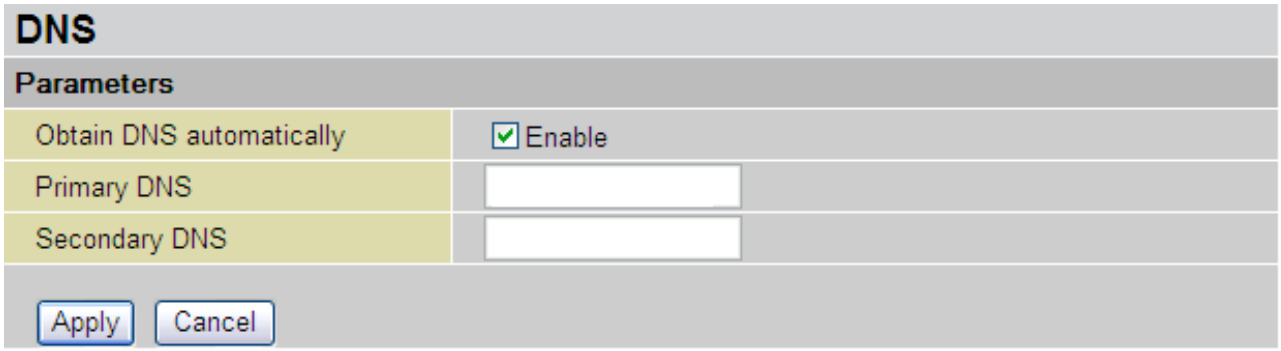
Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

DNS



A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com and an IP address. An IP address is a 32-bit number in the form of *xxx.xxx.xxx.xxx*, for example 192.168.1.254. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

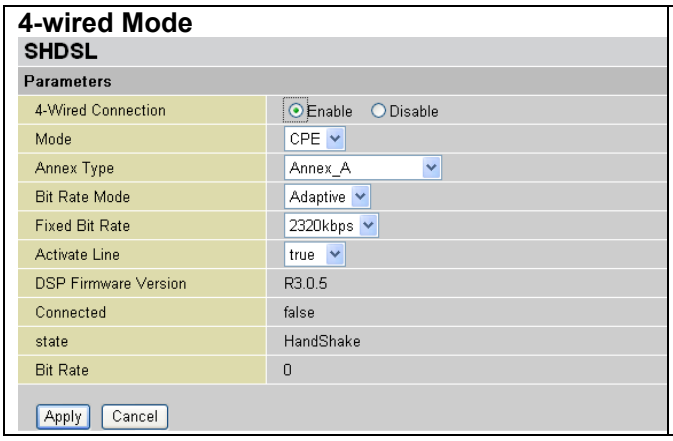
You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon, check the **Enable** box. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave the configuration field blank.

Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address manually.

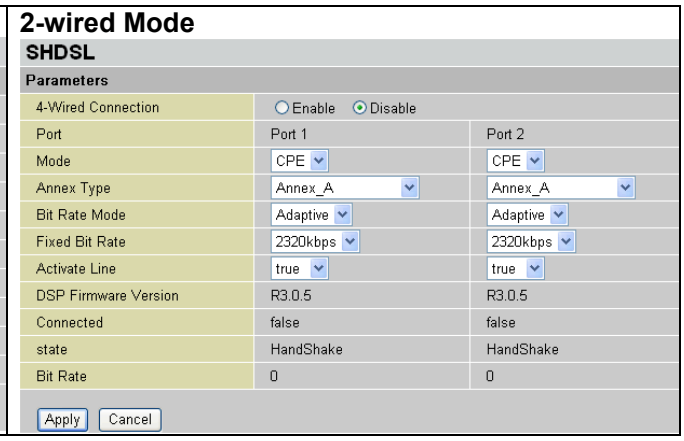
If you choose one of the other three protocols _ RFC1483 Routed/Bridged and IPoA check with your ISP, it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS of your PC to the LAN IP address of this router.

SHDSL

4-wired Mode



2-wired Mode



4-Wired Connection: MICHELANGELO SHDSL supports either 2-wire and 4-wires SHDSL connection. Activate the device to 4-wired by enabling the function; otherwise, disable it to be used as 2-wire mode connection.

Note: When select **2-wired mode**, only **Port 1** settings need to be configured and the SHDSL (RJ-11 cable) must be connected to **LINE 1** on the back of the device.

Mode: The SHDSL device can function as a CPE (Customer Premises Equipment) or CO (Central Office). Select CPE mode when the Michelangelo SHDSL is connecting to your ISP.

Back – to –back: it is a direct connection between two SHDSL devices which one is set to CPE and the other is CO by using a standard RJ-11 telephone cable.

Annex Type: It is the DSL operating mode standard. Select Annex A or Annex B to support up to 2.3Mpbs (for 2-wired mode) and 4.6Mpbs (for 4-wired mode). Select other annex such as Annex B_ANFP / Annex A_B_ANFP, you may consult with your ISP first.

Back – to –back: to be sure the Annex type is the same on the MICHELANGELO SHDSL and the remote router.

Bit Rate Mode: The mode selections are Adaptive and Fixed. Selecting the Adaptive mode, the best connection rate will be automatically negotiated with the CO / ISP. Selecting the Fixed mode, the connection rate will be fixed to the specific fixed bit rate selected with the CO / ISP.

Fixed Bit Rate: Specify the fix transfer rate when Fixed Mode is selected. Specify the maximum transfer rate when Adaptive Mode is selected. Bit Rate range is from 72kbps ~ 2368kbps.

Activate Line: Line active **true** is set by default. Select **false** to disable and **true** to enable SHDSL SHDSL connection

Note: Once Active Line is selected as **false**, you must enable the Active Line to **true** again and click Apply button to reactivate SHDSL connection.

DSP FirmwareVersion: Display the SHDSL line code firmware version.

Connected: Display current SHDSL line sync status.

State: Display current SHDSL line status.

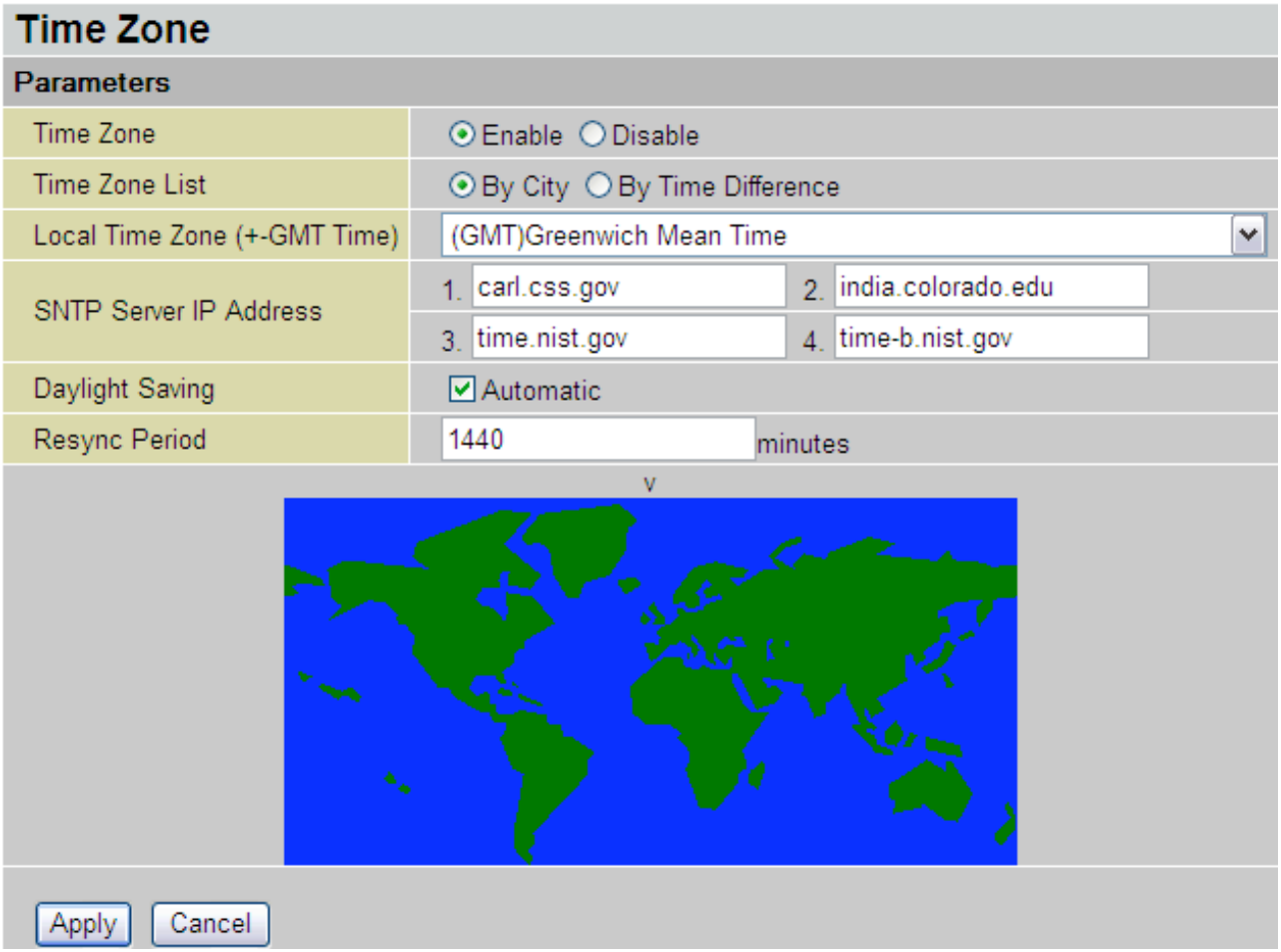
Bit Rate: Display SHDSL line synch speed rate.

Click **Apply** button to apply your changes

System

Here are items within the **System** section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart** and **User Management.**

Time Zone

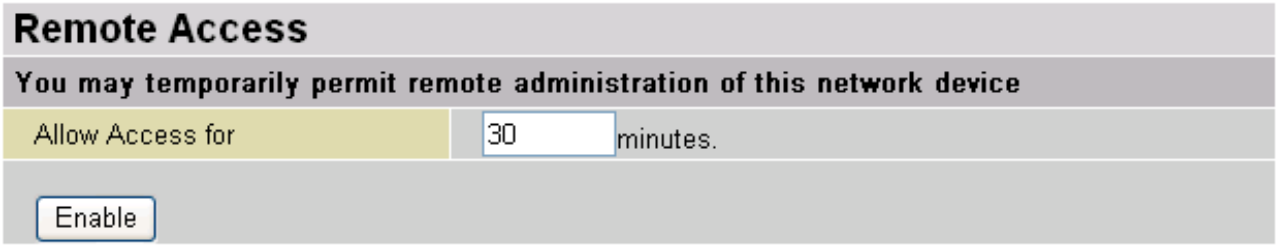


The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Daylight Saving is also known as ***Summer Time Period.*** Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check **Automatic** box to auto set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

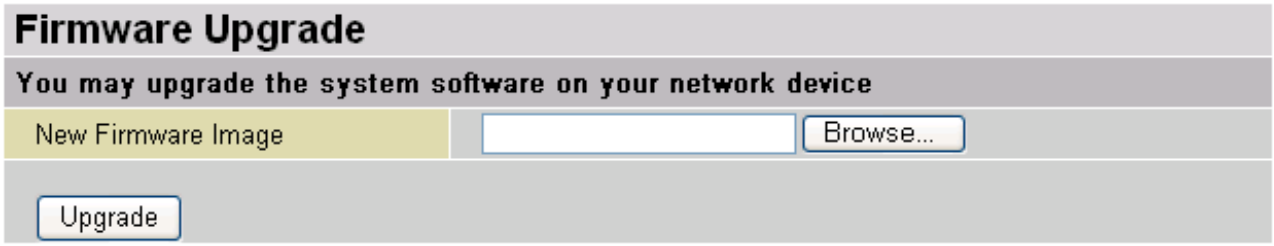
Remote Access



To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router will permit remote access for and click **Enable.** You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

If you wish to permanently enable remote access, choose a time period of **0** minutes.

Firmware Upgrade



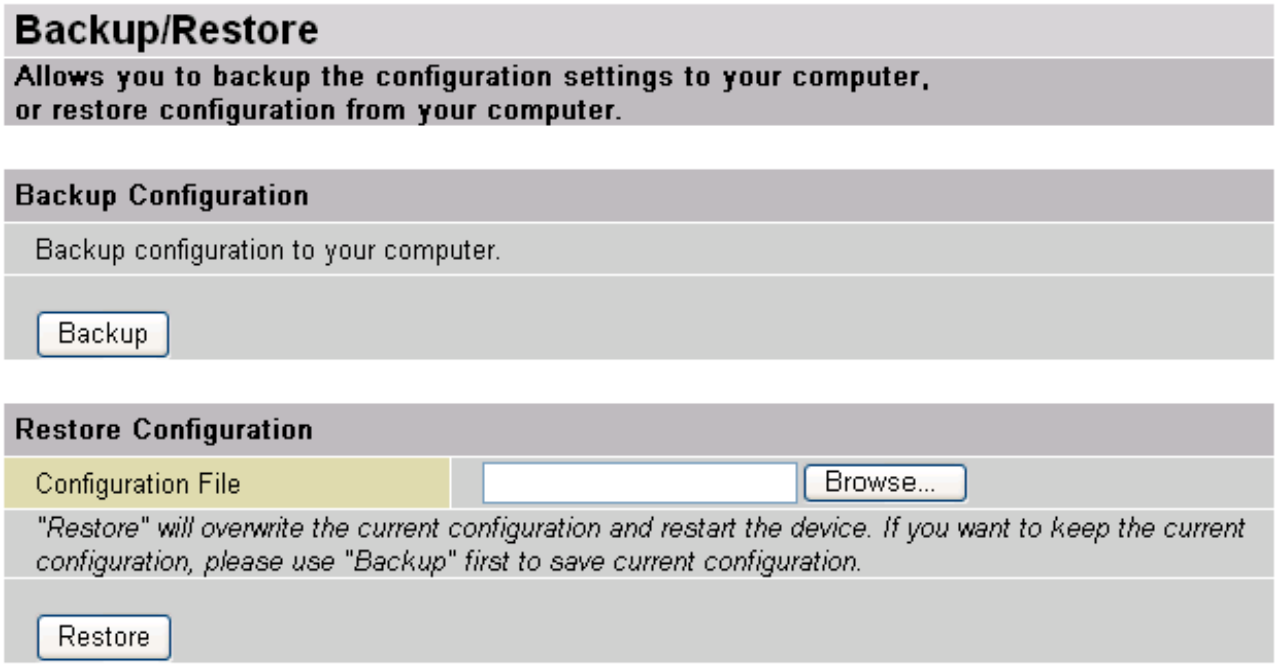
Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

Warning

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore


Backup/Restore
Allows you to backup the configuration settings to your computer,
or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse...
"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

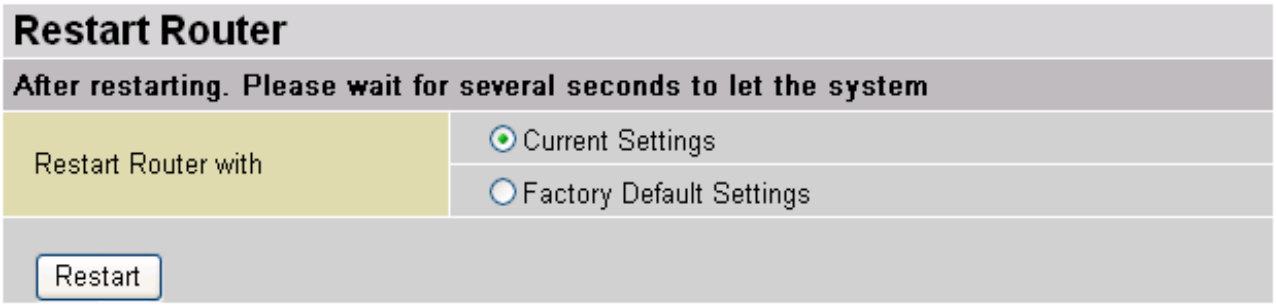
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

After selecting the settings file you wish to use, pressing **Restore** will load those settings into the router.

Restart Router

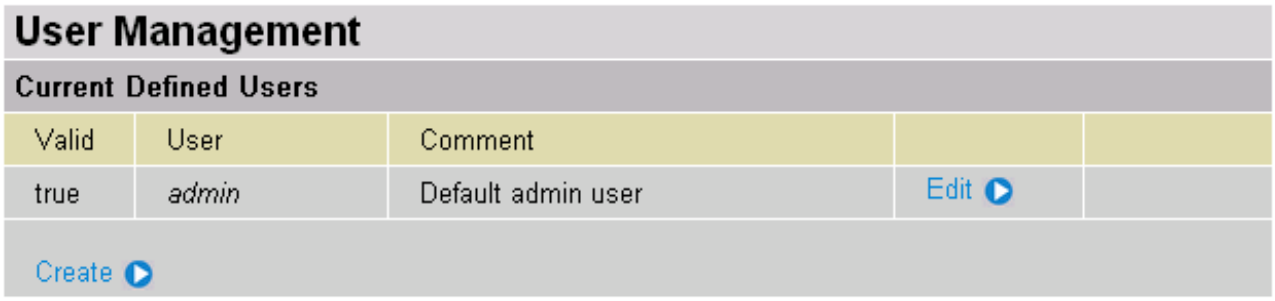
Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

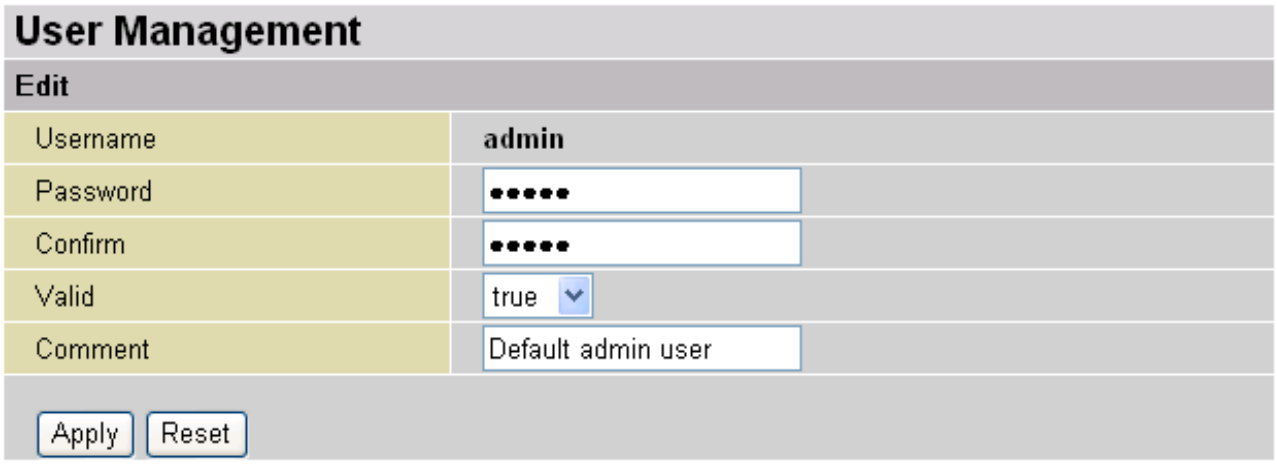
You may also hardware reset your router to factory settings by holding the **RESET** pinhole button on the back panel of the router for more than 6 seconds whilst the router is turned on.

User Management



In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Create** new users who are able to access the device's configuration interface. Once you have clicked on **Edit,** you are shown the following options:

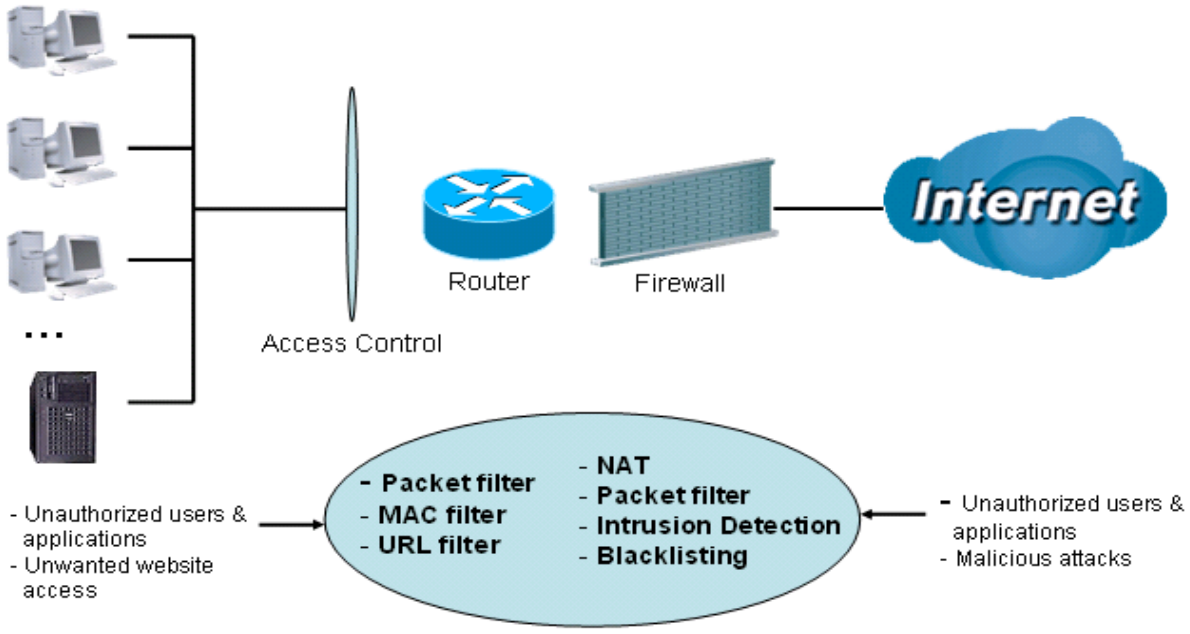


You can change the user's **password**, whether their account is active and **Valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however, you can delete any other created accounts by clicking **Delete** when editing the user.

You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT, the router acts as a "natural" Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.



Firewall & Filter

Firewall: Prevents access from outside your network. The router provides three levels of security support:

NAT natural firewall: This masks LAN users' IP addresses which is invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when NAT function is enabled.

When using Virtual Servers your PCs will be exposed to the degree specified in your Virtual Server settings provided the ports specified are opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

Access Control: Prevents access from PCs on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the Internet.

URL Filter: To block PCs on your local network from unwanted websites.

Here are items under the **Firewall** section: **General Settings, Packet Filter, Intrusion Detection, URL Filter, IM/P2P Blocking** and **Firewall Log.**

General Settings

You can choose not to enable Firewall, you will not able to add filter rules by yourself in the Packet Filter, or enable the Firewall using preset filter rules and modify the packet filter rules as required. The Packet Filter is used to filter packets based-on Applications (Port) or IP addresses.

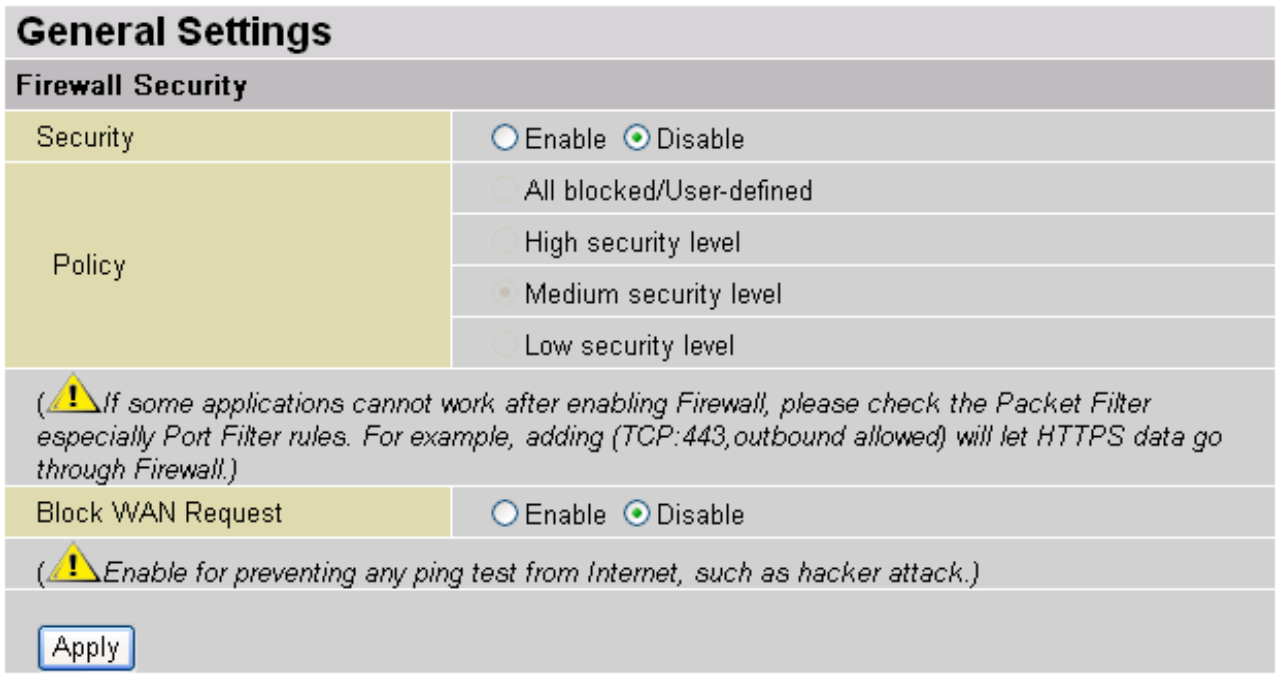
There are four options when you enable the Firewall, they are:

- **All blocked/User-defined**: no pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.
- **High/Medium/Low security level:** the predefined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

Select either **High, Medium** or **Low security level** to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall functionality is the same for all levels; it is only the list of preset port filters that changes between each setting. For more detailed on level of preset port filter information, refer to **Table 1: Predefined Port Filter**.

Note: The changes or added custom filters on a previous security level will be remembered whenever newer security level is selected. There is no need to reconfigure all settings again if switching back to the previous level.

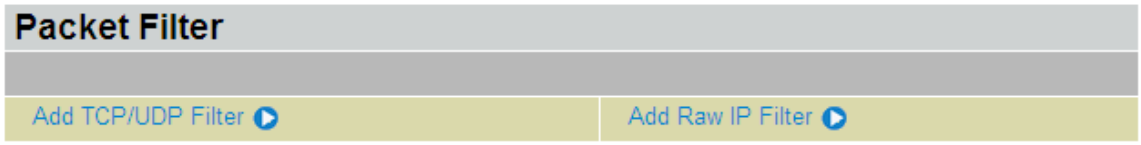
The "**Block WAN Request**" is a stand-alone function and not relate to whether security enable or disable. Mostly it is for preventing any scan tools from WAN site by hacker.


General Settings
Firewall Security
Security
Enable
Disable
Policy
All blocked/User-defined
High security level
Medium security level
Low security level
(If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)
Block WAN Request
Enable
Disable
(Enable for preventing any ping test from Internet, such as hacker attack.)
Apply

Any remote user who is attempting to perform this action may result in blocking all the accesses to configure and manage of the device from the Internet.

Packet Filter

This function is only available when the Firewall is enabled and one of these four security levels is chosen (All blocked, High, Medium and Low). The predefined port filter rules in the Packet Filter must modify accordingly to the level of Firewall, which is selected. See **Table1: Predefined Port Filter** for more detailed information.



Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
lei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
lei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
lei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
lei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
lei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete
lei_smtp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Block Allow	Edit	Delete
lei_pop3	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Block Allow	Edit	Delete

Example: Predefined Port Filters Rules

The predefined port filter rules for High, Medium and Low security levels are listed. See Table 1.

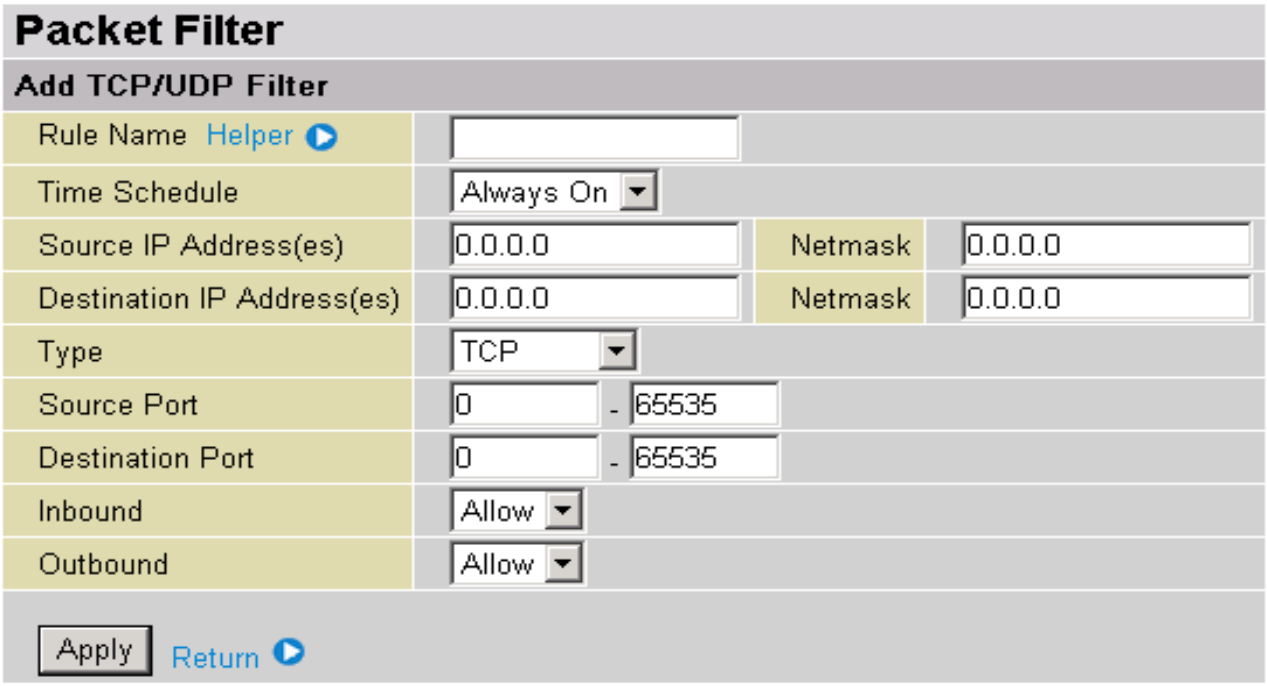
Note: Firewall – All Blocked/User-defined, you must define and create the port filter rules yourself. No predefined rule is being preconfigured.

Table 1: Predefined Port Filter

Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP /SNTP (123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy (8080)	TCP(6)	8080	8080	NO	YES	NO	YES	N/A	N/A
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN; **Outbound:** LAN to Internet.
YES: Allowed; **NO:** Blocked; **N/A:** Not Applicable

Packet Filter – Add TCP/UDP Filter



Rule Name: Users-define description to identify this entry or click Helper to select existing predefined rules. The maximum name length is 32 characters.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Selecting the **Subnet Mask** of the IP address range you wish to allow/block the traffic to or form; set IP address and Subnet Mask to **0.0.0.0** to inactive the Address-Filter rule.

Tip: To block access, to/from a single IP address, enter that IP address as the **Host IP Address** and use a **Host Subnet Mask** of "255.255.255.255".

Type: It is the packet protocol type used by the application, select among from **TCP** or **UDP** or both of **TCP/UDP**.

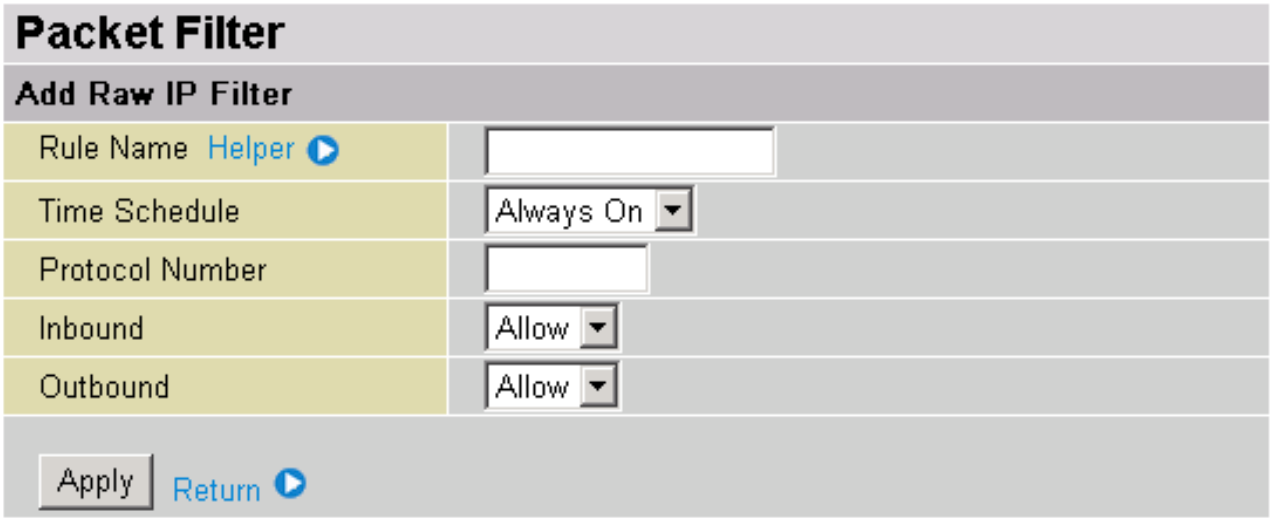
Source Port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535.** It is recommended that this option be configured by an advanced user.

Destination Port: This is the Port or Port Ranges that defines the application.

Inbound / Outbound: Select **Allow** or **Block** the access to the Internet (**"Outbound"**) or from the Internet (**"Inbound"**).

Click **Apply** button to apply your changes.

Packet Filter – Add Raw IP Filter



Rule Name: Users-define description to identify this entry or click Helper to select existing predefined rules.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section

Protocol Number: Insert the port number, i.e. GRE 47.

Inbound / Outbound: Select **Allow** or **Block** the access to the Internet (**"Outbound"**) or from the Internet (**"Inbound"**).

Click **Apply** button to apply your changes.

Example: Configuring your firewall to allow for a publicly accessible web server on your LAN

The predefined port filter rule for HTTP (TCP port 80) is the same no matter whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

As you can see from the diagram below, when the firewall is enabled with one of the three presets (Low/Medium/High), inbound HTTP access is not allowed which means remote access through HTTP to your router is not allowed.

Note: Inbound indicates accessing from Internet to LAN and Outbound is from LAN to the Internet.

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
mei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete
mei_smtp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Block Allow	Edit	Delete
mei_pop3	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Block Allow	Edit	Delete
mei_nntp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 119 ~ 119	Block Allow	Edit	Delete

Configuring Packet Filter:

1. Click **Port Filters**. You will then be presented with the predefined port filter rules screen (in this case for the low security level), shown below:
   Note: You may click Edit the predefined rule instead of Delete it. This is an example to show to how you add a filter on your own.

Packet Filter

Add TCP/UDP Filter | Add Raw IP Filter

Packet Filter Rules

Click Delete

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
mei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete

2. Click **Delete** to delete the existing HTTP rule.
3. Click **Add TCP/UDP Filter**.

Packet Filter

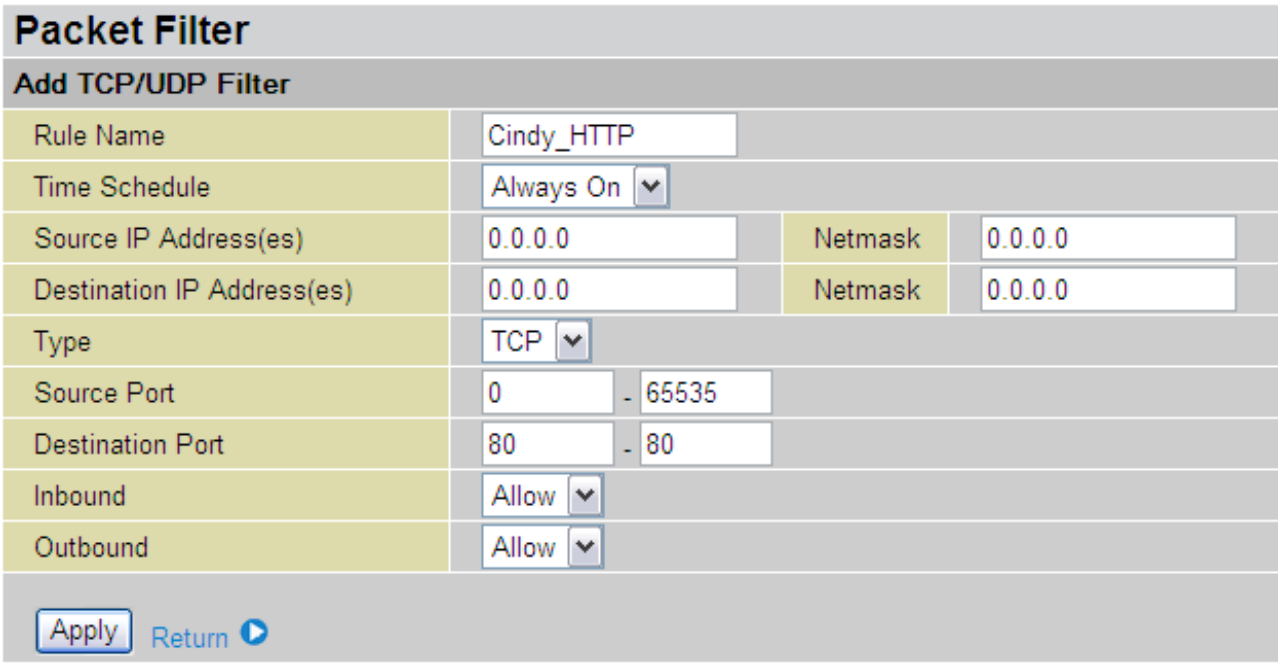
Click Add TCP/UDP Filter

Add TCP/UDP Filter | Add Raw IP Filter

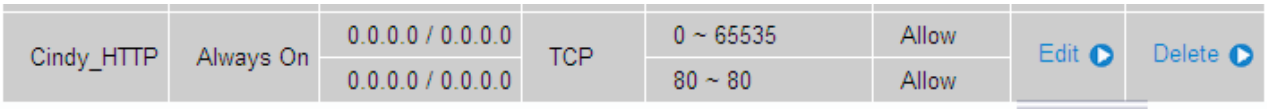
4. Input the Rule Name, Time Schedule, Source/Destination IP, Type, Source/Destination Port, Inbound and Outbound.

   ***Example*:**

   Application: *Cindy_HTTP*
   Time Schedule: *Always On*
   Source / Destination IP Address (es): *0.0.0.0* ***(I do not wish to active the address-filter, instead I use the port-filter)***
   Type: *TCP (Please refer to Table1: Predefined Port Filter)*
   Source Port: *0-65535* ***(I allow all ports to connect with the application))***
   Redirect Port: *80-80* ***(This is Port defined for HTTP)***
   Inbound / Outbound: *Allow*

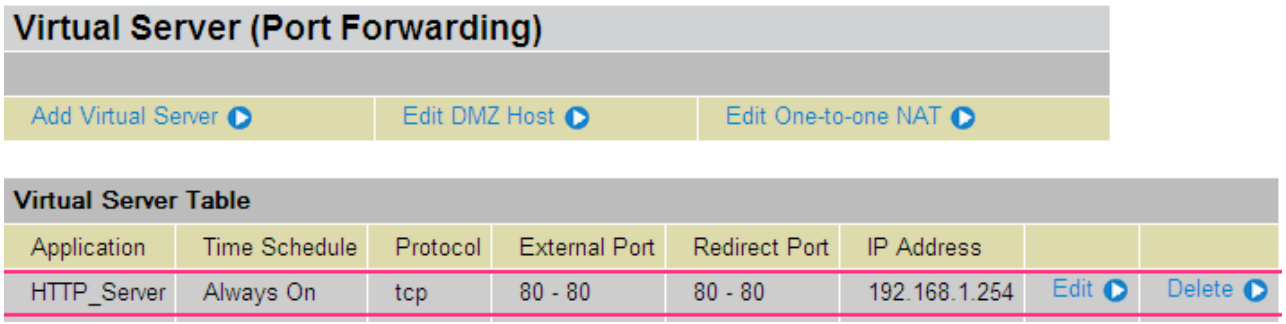


5. The new port filter rule for HTTP is shown below:



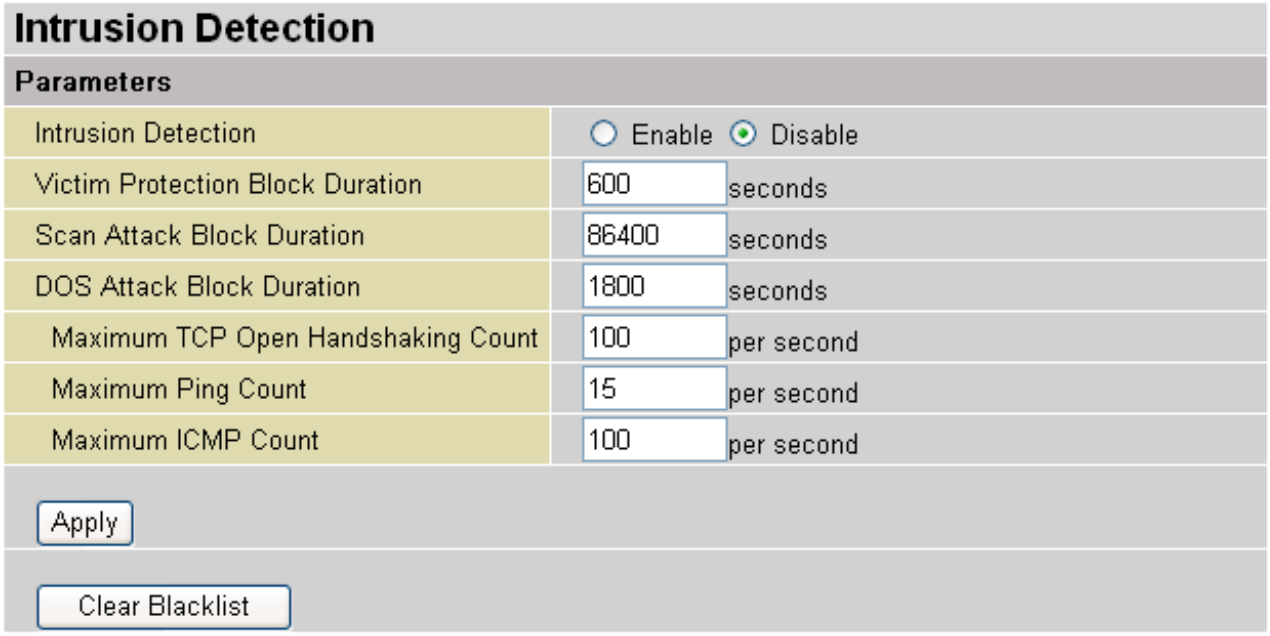
6. Configure your Virtual Server (“port forwarding”) settings so that incoming HTTP requests on port 80 will be forwarded to the PC running your web server:

Note: For how to configure the HTTP in Virtual Server, go to Add Virtual Server in Virtual Server section for more details.



.

Intrusion Detection



The router's *Intrusion Detection System* (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified as the **Block Duration**. The default setting for this function is false (disabled). Some attack types are denied immediately without using the Blacklist function, such as *Land attack* and *Echo/CharGen scan*.

Intrusion Detection: If enabled, IDS will block Smurf attack attempts. Default is false.

Block Duration:

- **Victim Protection Block Duration**: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.
- **Scan Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.
- **DoS Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

Max TCP Open Handshaking Count: This is a threshold value to decide whether a *SYN Flood* attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an *ICMP Echo Storm* is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an *ICMP flood* is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

For *SYN Flood*, *ICMP Echo Storm* and *ICMP flood*, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

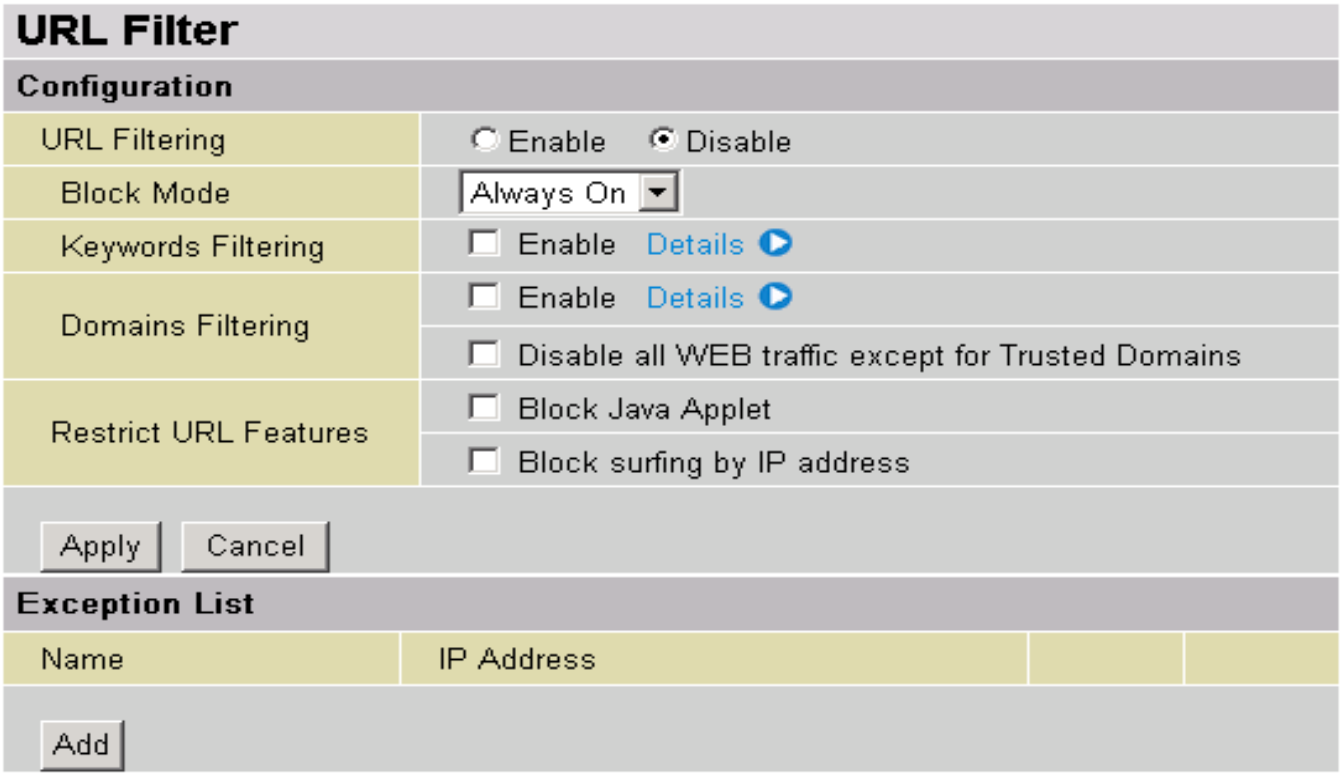
Table 2: Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Src Port: Source Port
Dst Port: Destination Port
Dst IP: Destination IP

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Enable/Disable: To enable or disable URL Filter feature.

Block Mode: A list of the modes that you can choose to check the URL filter rules.

⊙ **Disabled:** No action will be performed by the Block Mode.

⊙ **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.

⊙ **TimeSlot1 ~ TimeSlot16:** It is self-defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called "advertisement.gif"). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is http://www.abc.com/abcde.html, it will be dropped as the keyword "abcde" occurs in the URL.

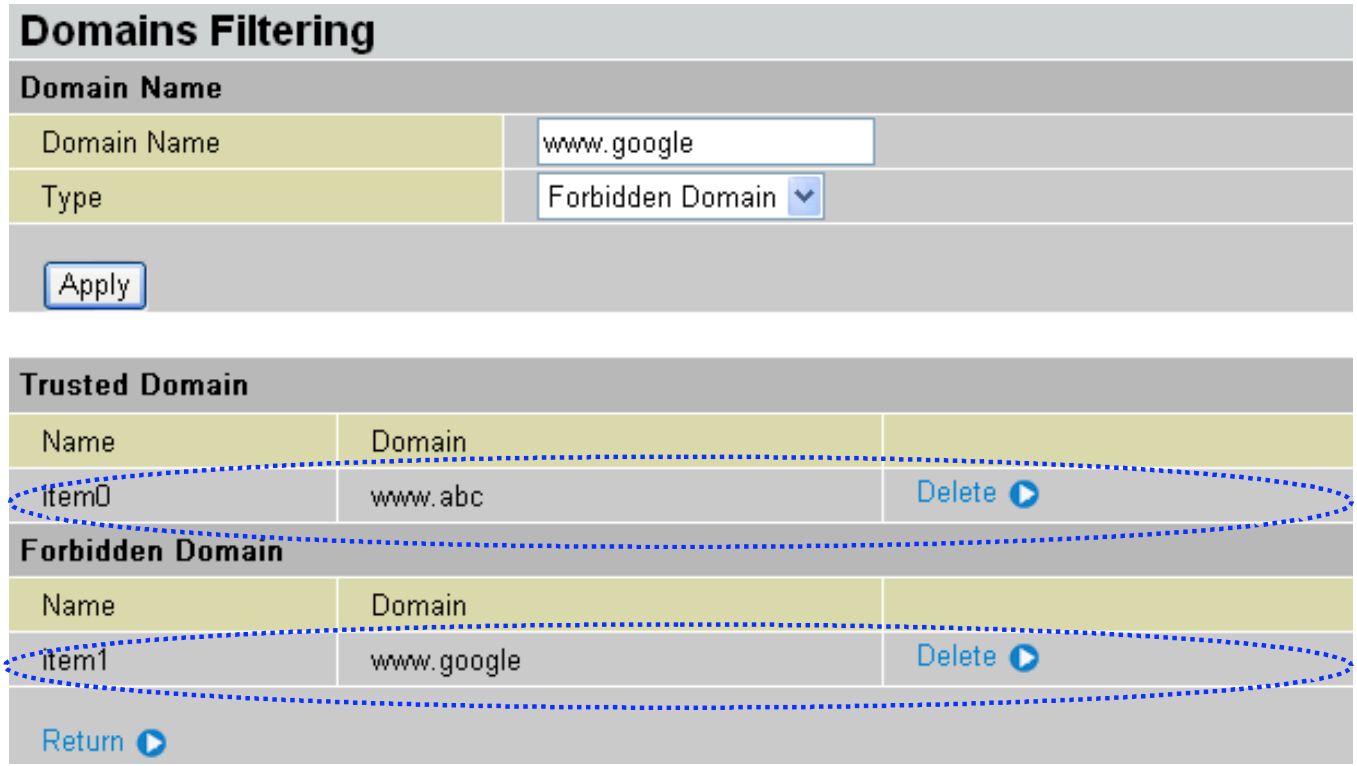
Domains Filtering: This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be

dropped.

3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name, shall be specified. For example to block traffic to www.google.com.au, enter “www.google” or “www.google.com”

In the example below, the URL request for www.abc.com will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.google or www.google.com will be dropped, because www.google is in the forbidden list.



Example: Andy wishes to disable all WEB traffic except for ones listed in the trusted domain, which would prevent Bobby from accessing other web sites. Andy selects both functions in the *Domain Filtering* and thinks that it will stop Bobby. But Bobby knows this function, *Domain Filtering*, ONLY disables all WEB traffic except for **Trusted Domain,** BUT not its **IP address.** If this is the situation, **Block surfing by IP address** function can be handy and helpful to Andy. Now, Andy can prevent Bobby from accessing other sites.

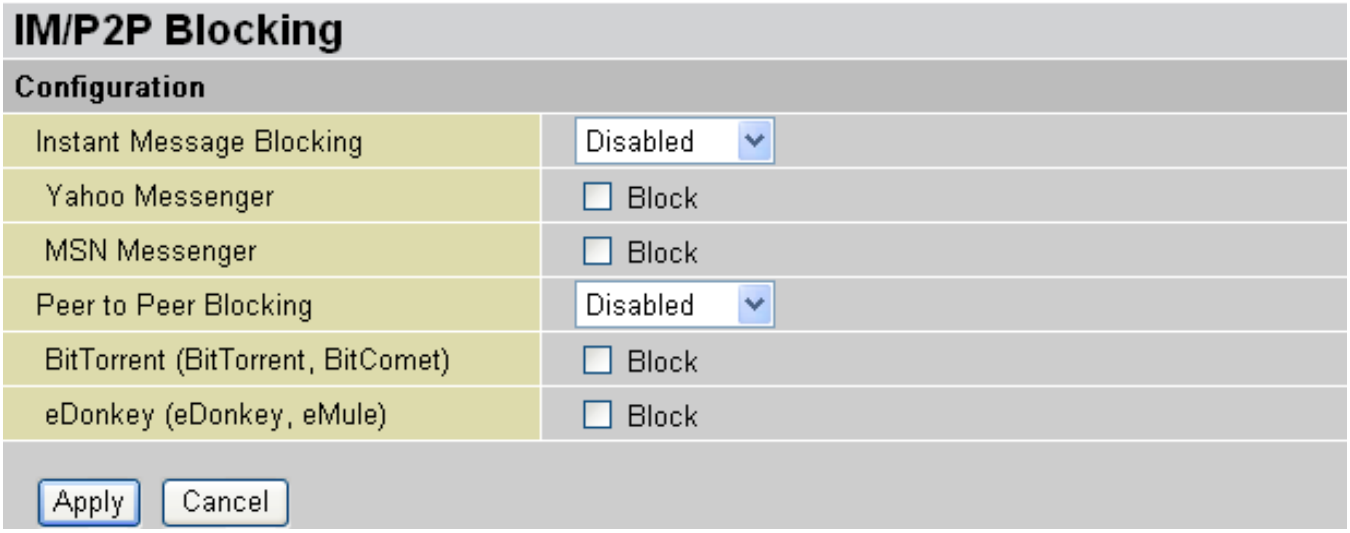
Restrict URL Features: This function enhances the restriction to your URL rules.

⊙ **Block Java Applet:** This function can block Web content that includes the Java Applet. It is to prevent someone who wants to damage your system via standard HTTP protocol.

⊙ **Block surfing by IP address:** Preventing someone who uses the IP address as URL for skipping Domains Filtering function. Activates only and if Domain Filtering enabled.

IM / P2P Blocking

IM, short for Instant Message, is required to use client program software that allows users to communicate, in exchanging text message, with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of computer users who share file to specific groups of people across the Internet. Both Instant Message and Peer-to-peer applications make communication faster and easier but your network can become increasingly insecure at the same time. Digicom's IM and P2P blocking helps users to restrict LAN PCs to access to the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.



Instant Message Blocking: The default is set to **Disabled.**

⊙ **Disabled:** Instant Message blocking is not triggered. No action will be performed.

⊙ **Always On:** Action is enabled.

⊙ **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Yahoo/MSN Messenger: Check the box to block either or both Yahoo or/and MSN Messenger. To be sure you enabled the *Instant Message Blocking* first.

Peer to Peer Blocking: The default is set to **Disabled.**

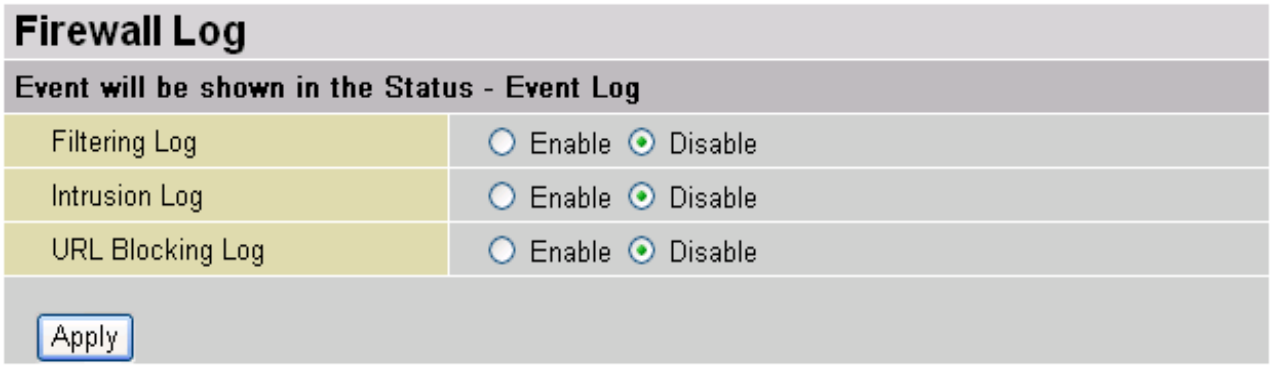
⊙ **Disabled:** Instant Message blocking is not triggered. No action will be performed.

⊙ **Always On:** Action is enabled.

⊙ **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

BitTorrent / eDonkey: Check the box to block either or both Bit Torrent or/and eDonkey. To be sure you enabled the *Peer to Peer Blocking* first.

Firewall Log



Firewall Log display log information of any unexpected action with your firewall settings.

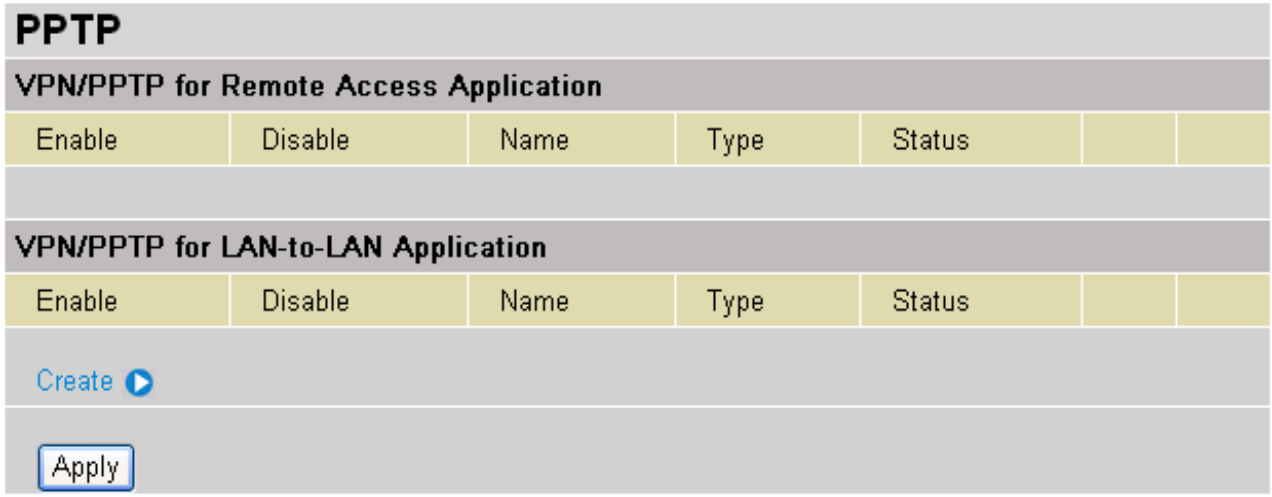
Check the **Enable** box to activate the logs.

Log information can be seen in the **Status – Event Log** after enabling.

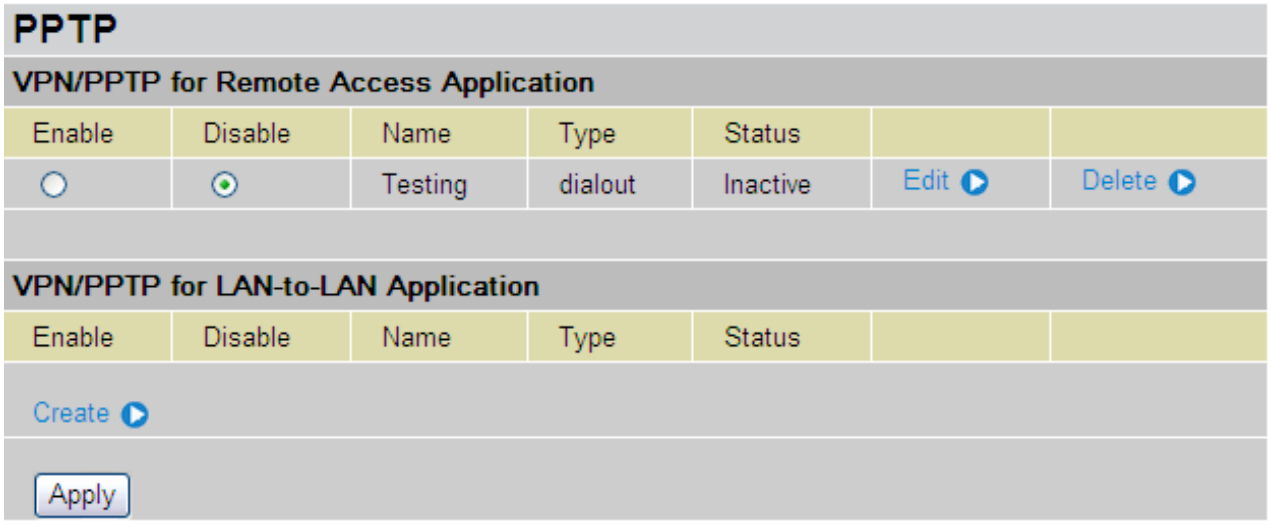
VPN - Virtual Private Networks

Virtual Private Networks is ways to establish secured communication tunnels to an organization's network via the Internet. Your router supports three main types of VPN (Virtual Private Network), **PPTP**, **IPSec** and **L2TP.**

PPTP (Point-to-Point Tunneling Protocol)



There are two types of PPTP VPN supported; **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to configure a new VPN connection.



After you have created PPTP connection, account status will be displayed. (See example above).

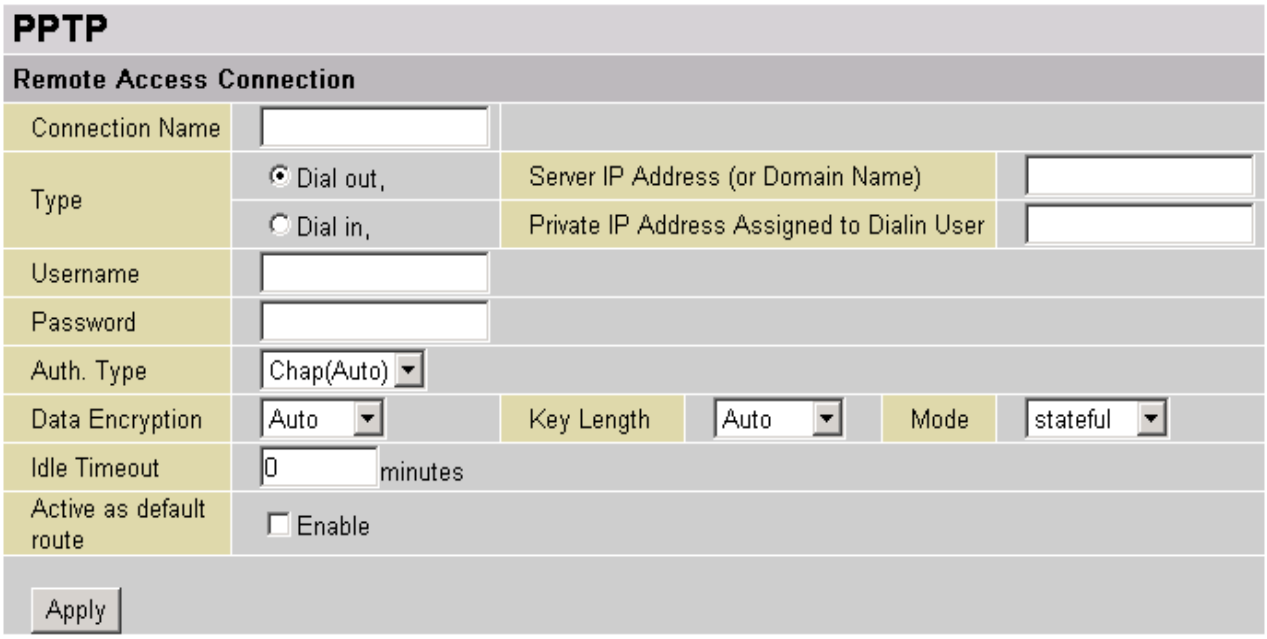
⊙ **Enable / Disable:** This function activates or deactivates the PPTP connection. To wish interrupting the tunnel, check **Disable** radio button and click **Apply** button to deactivate the connection.

Name: User-defined name of the connection.

Type: This refers to your router operates as a client or a server, **Dialout** or **Dialin** in respectively.

Status: It informs your PPTP tunnel connection condition.

PPTP Connection - Remote Access



Connection Name: User-defined name for the connection (e.g. “connection to office”).

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Domain Name)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

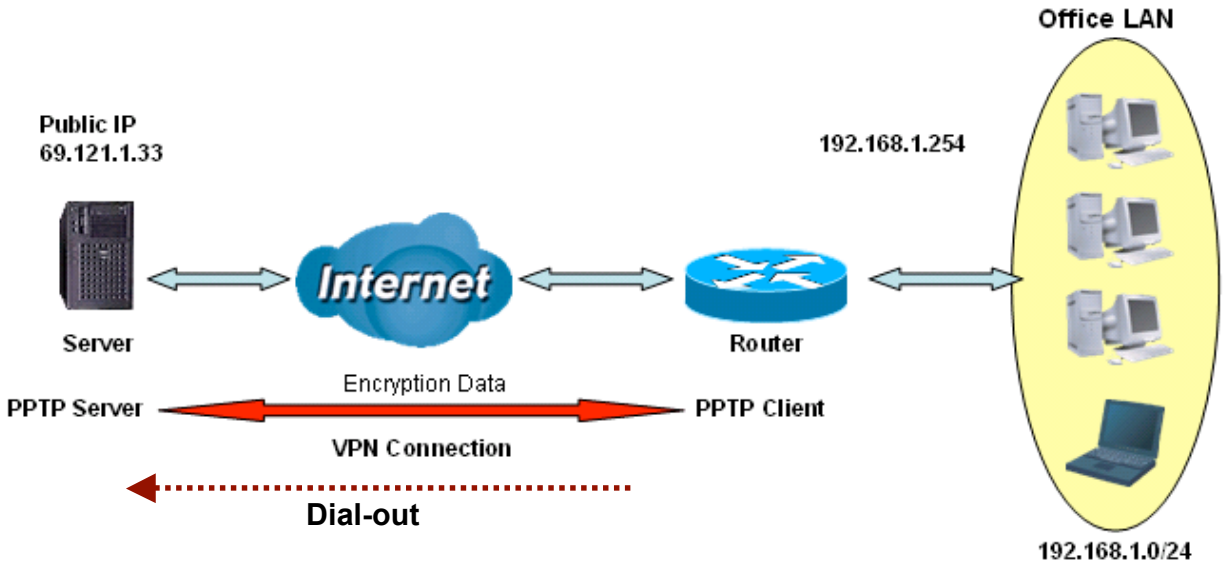
Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Click **Apply** button to apply your changes.

Example: Configuring a Remote Access PPTP VPN Dial-out Connection

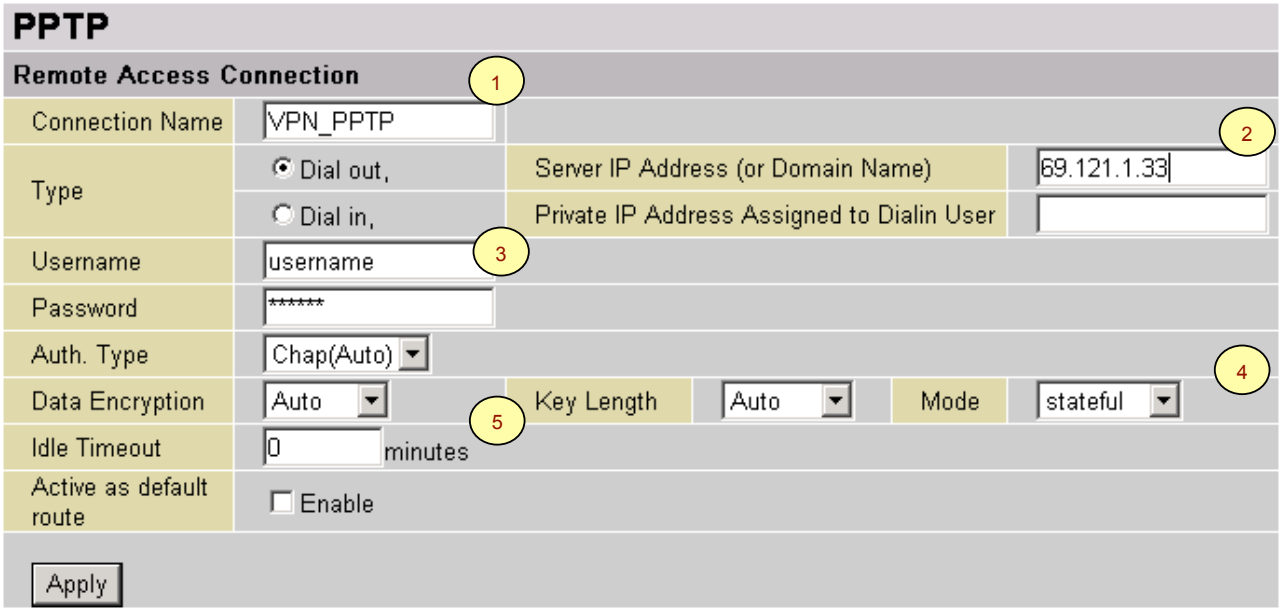
A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



PPTP VPN-Remote Access (Dial-out)

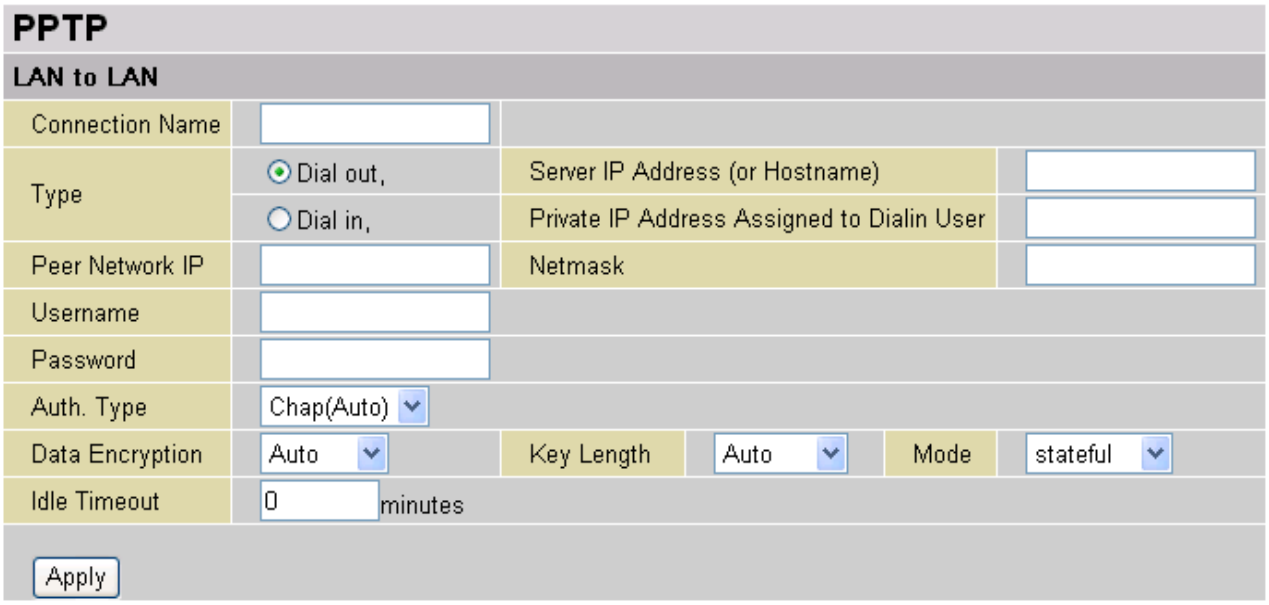
Configuring the PPTP VPN in the Office

You can either input the IP address (69.1.121.33 in this case) or hostname to reach the server.



Item	Function		Description
1	Connection Name	VPN_PPTP	Given name of PPTP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	An Dialed server IP
3	Username	username	A given username & password
	Password	123456	
4	Auth.Type	Chap (Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
5	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always on.

PPTP Connection - LAN to LAN



Connection Name: User-define description of the connection.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by the your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

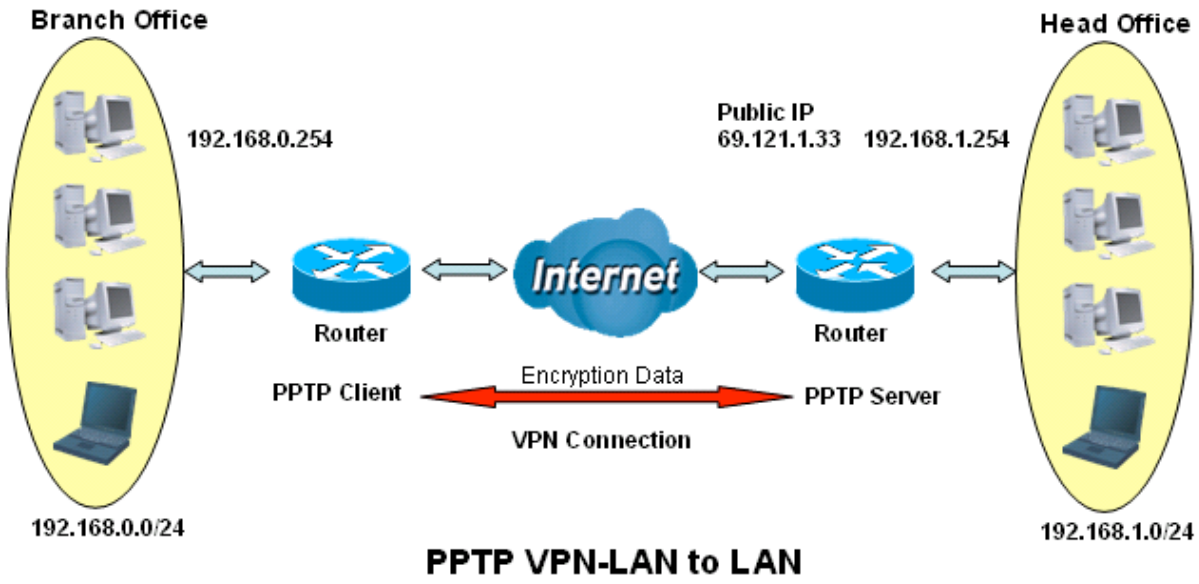
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Click **Apply** button to apply your changes.

Example: Configuring a PPTP LAN-to-LAN VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

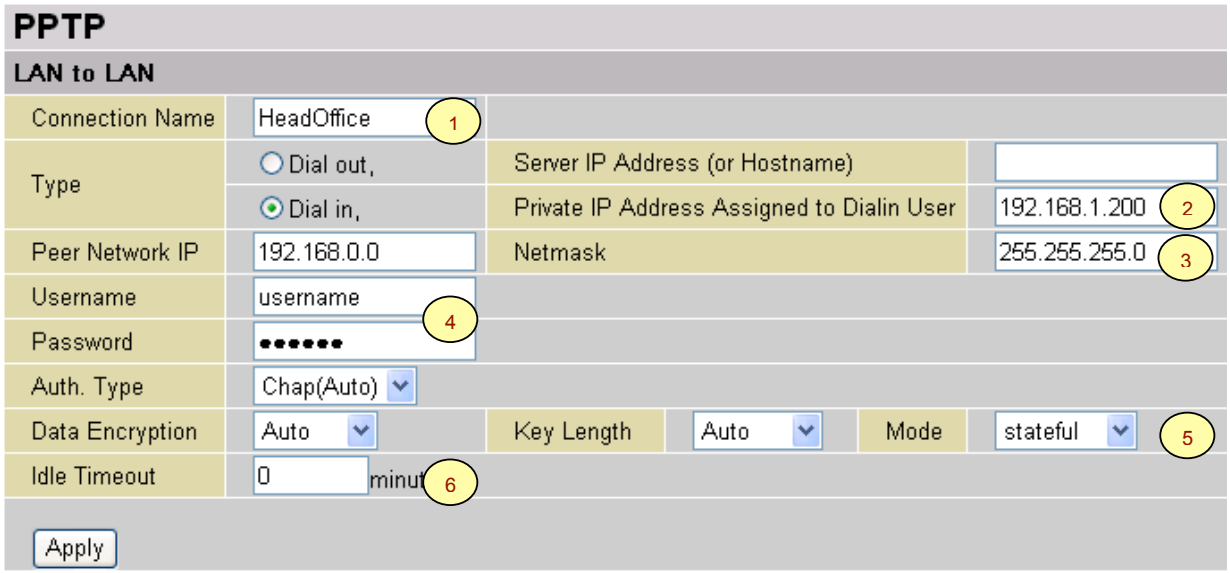


Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Configuring PPTP VPN in the Head Office

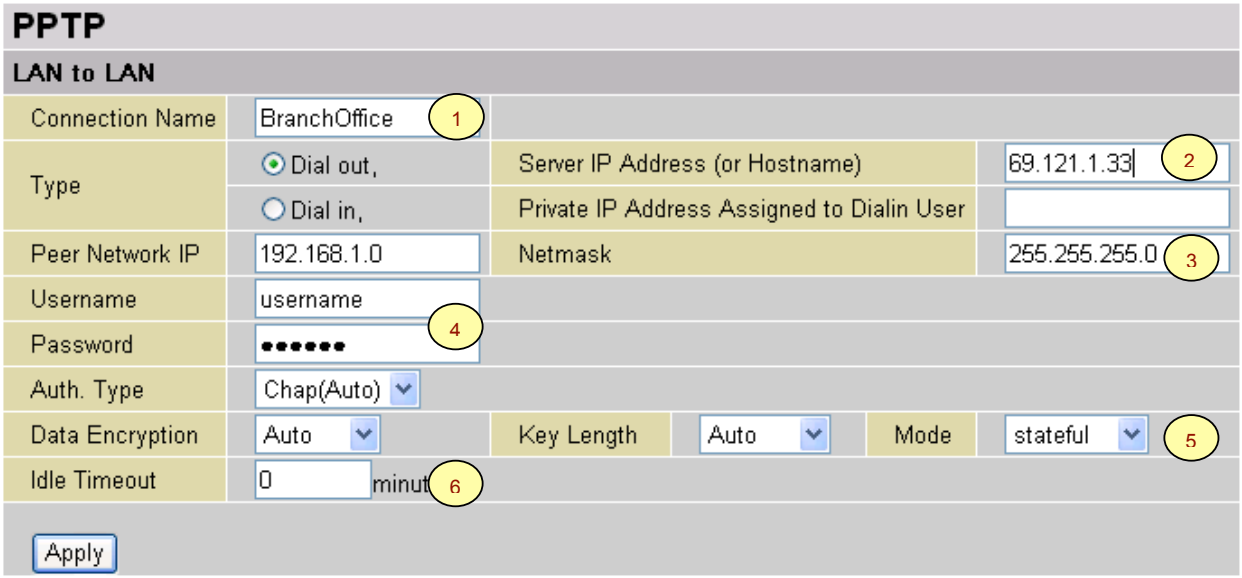
The IP address 192.168.1.201 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Connection Name	HeadOffice	Given a name of PPTP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	IP address assigned to branch office network
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.

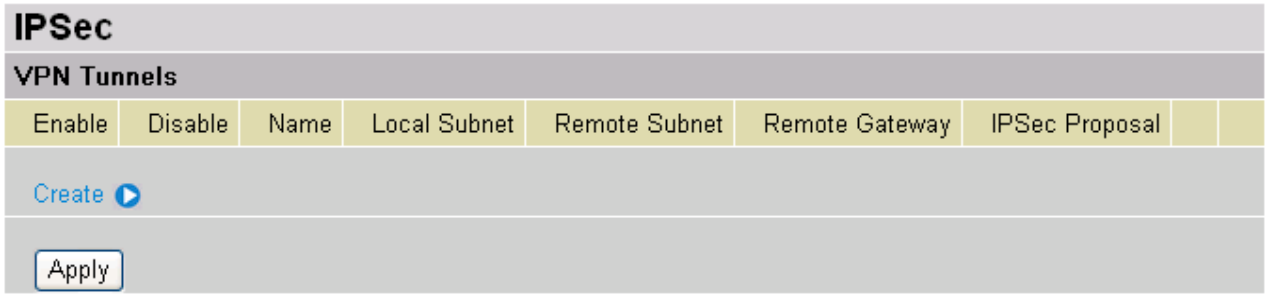
Configuring PPTP VPN in the Branch Office

The IP address 69.1.121.30 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.

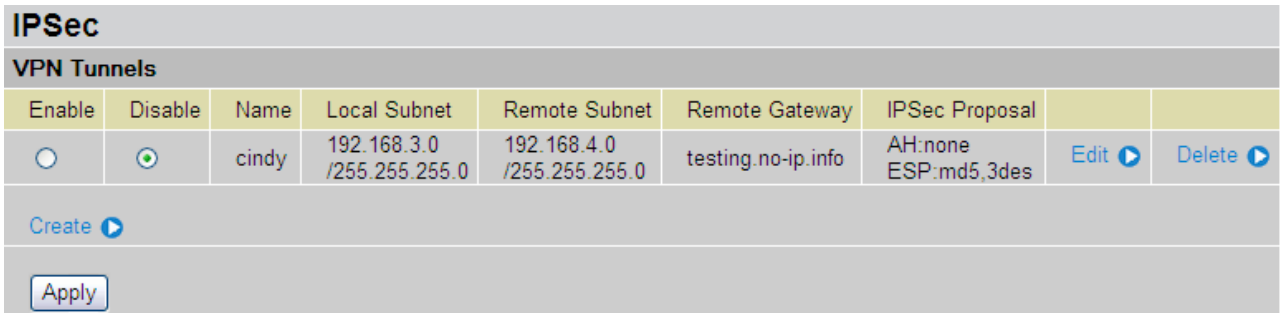


Item	Function		Description
1	Connection Name	BranchOffice	Given a name of PPTP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.

IPSec (IP Security Protocol)



Click **Create** to create a new IPSec VPN connection account.



After you have created the IPSec connection, account information will be displayed. (See example above).

⊙ **Enable / Disable:** This function activates or deactivates the IPSec connection. To wish interrupting the tunnel, check **Disable** radio button and click **Apply** button to deactivate the connection.

Name: This is the user-defined name of the connection.

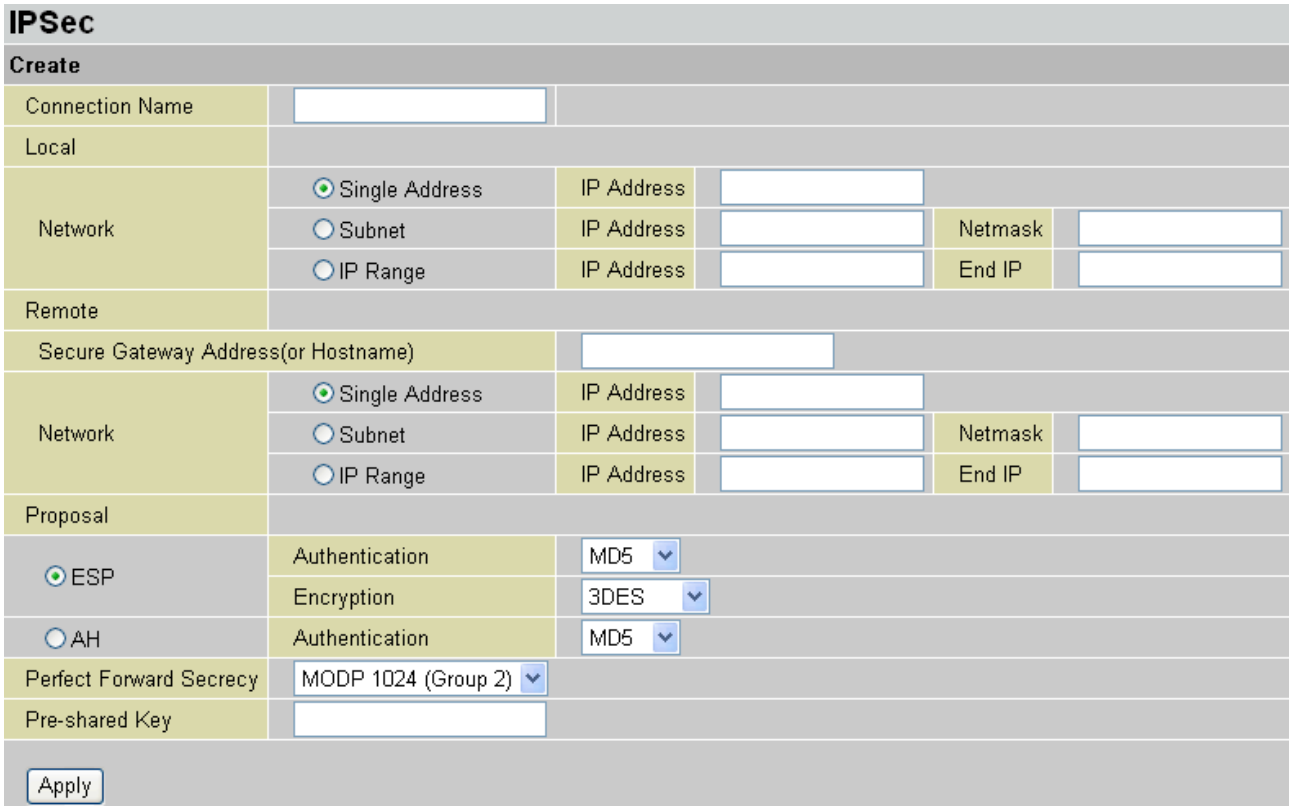
Local Subnet: Displays IP address and subnet of the local network.

Remote Subnet: Displays IP address and subnet of the remote network.

Remote Gateway: This is the IP address or Domain Name of the remote VPN device that is connected and established a VPN tunnel.

IPSec Proposal: This is selected IPSec security method.

IPSec VPN Connection



Connection Name: User-defined name for the connection (e.g. “connection to office”).

Local Network: Set the IP address, subnet or address range of the local network.

- **Single Address:** The IP address of the local host.
- **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).
- **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10.

Remote Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Remote Network: Set the IP address, subnet or address range of the remote network.

Proposal: Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128_bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160_bit hash.

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES**, **AES (128, 192 and 256)** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to

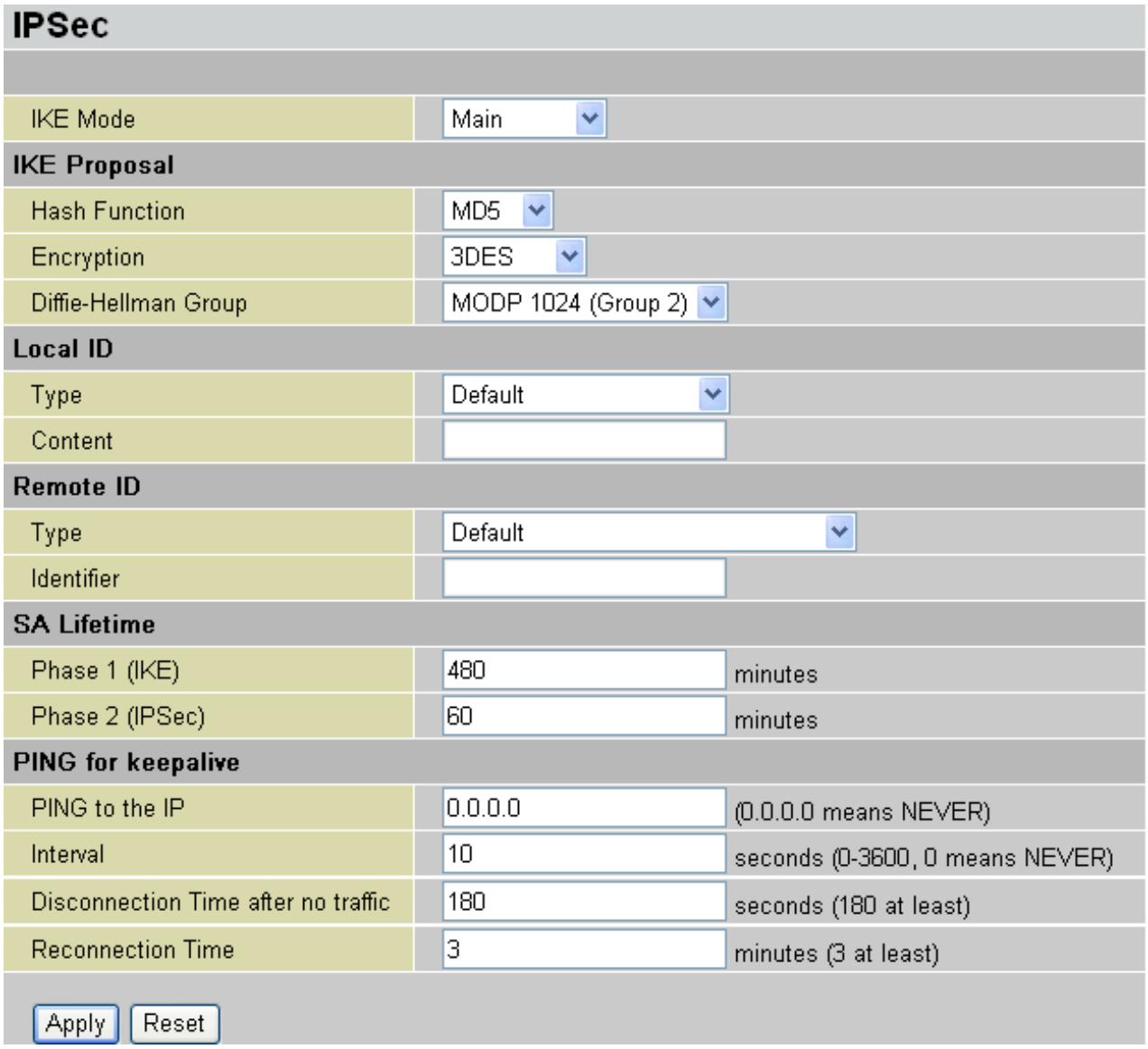
change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Select the **Apply** button to apply your changes.

Advanced Option

This function is only available after completed creating an IPSec account. Click **Advanced Option** to change the following settings:



IKE (Internet key Exchange) Mode: Select IKE mode to Main mode or Aggressive mode. This IKE provides secured key generation and key management.

IKE Proposal:

Hash Function: It is a Message Digest algorithm which coverts any length of a message into a unique set of bits. It is widely used MD5 (Message Digest) and SHA-1 (Secure Hash Algorithm) algorithms. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128_bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160_bit hash

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES** and **AES (128, 192 and 256)**. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Local ID:

- **Type:** Specify local ID type.
- **Content:** Input ID's information, like domain name www.ipsectest.com.

Remote ID:

- **Type:** Specify Remote ID type.
- **Identifier:** Input remote ID's information, like domain name www.ipsectest.com.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

- **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
- **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Ping to Keep Alive:

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Re-establish of this connection is required. Default setting is 0.0.0.0 which disables the function.

Interval: This sets the time interval between ***Pings to the IP*** function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

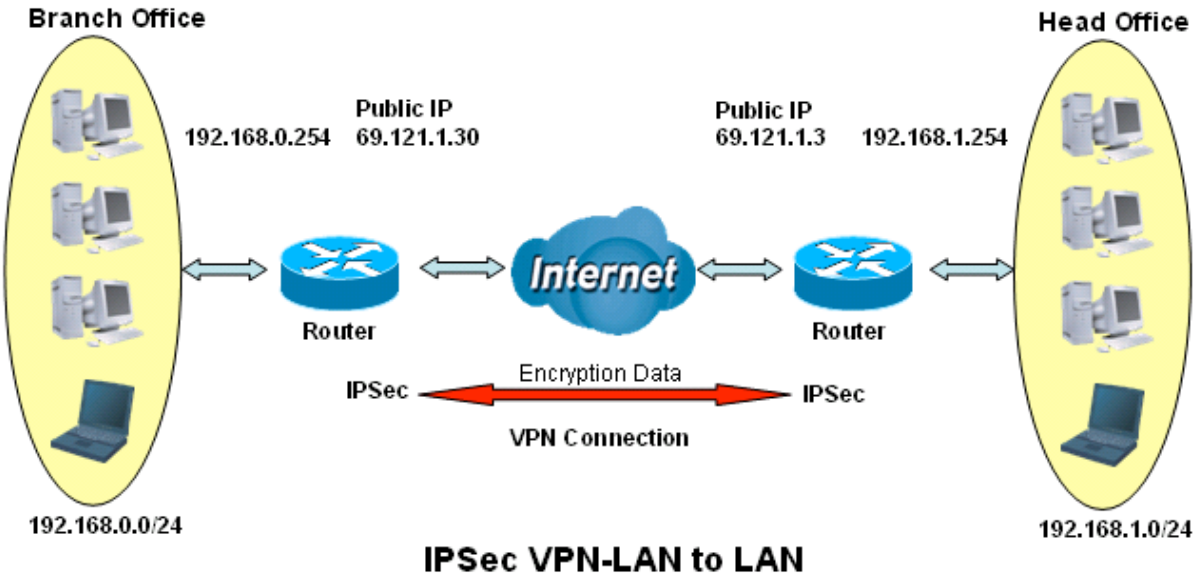
Ping to the IP	Interval (sec)	*Ping to the IP* Action
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the **Reconnection Time** set. **180 seconds** is minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. **3 minutes** is minimum time interval for this function.

Select the **Apply** button to update the settings.

Example: Configuring a IPSec LAN-to-LAN VPN Connection



IPSec VPN-LAN to LAN

Table 3: Network Configuration and Security Plan

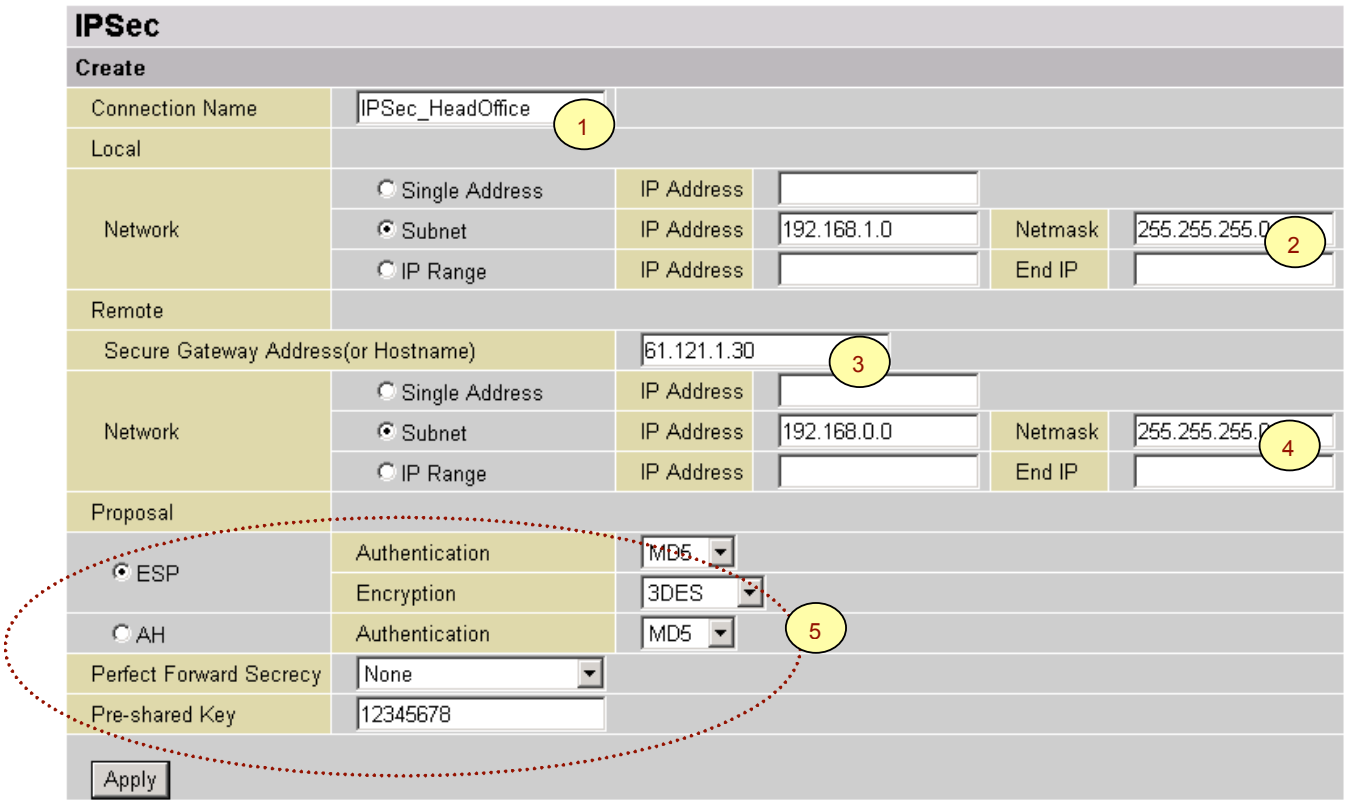
	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.1.121.30	69.1.121.3
Remote Network ID	192.168.1.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Connection Type	Tunnel mode	Tunnel mode
Security Algorithm	ESP:MD5 with AES	ESP:MD5 with AES

Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

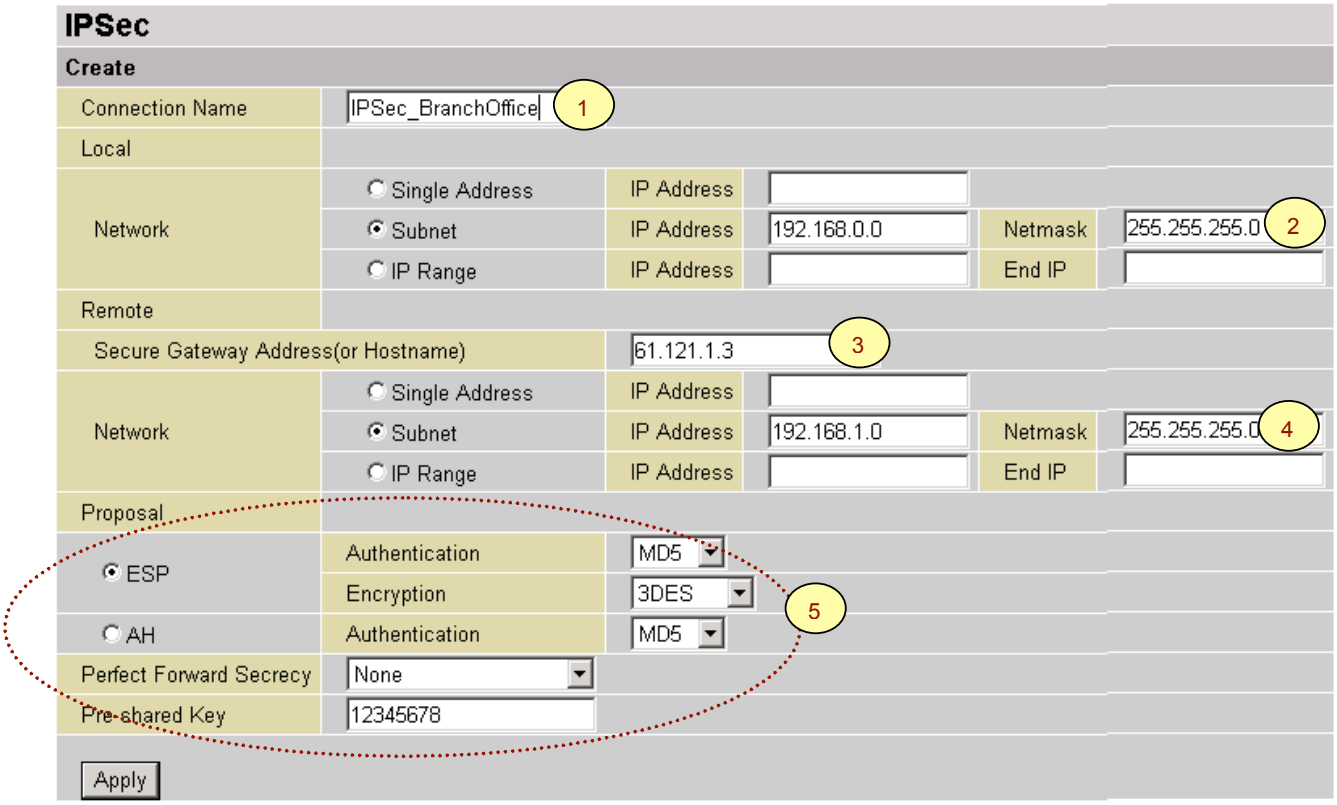
Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring IPSec VPN in the Head Office



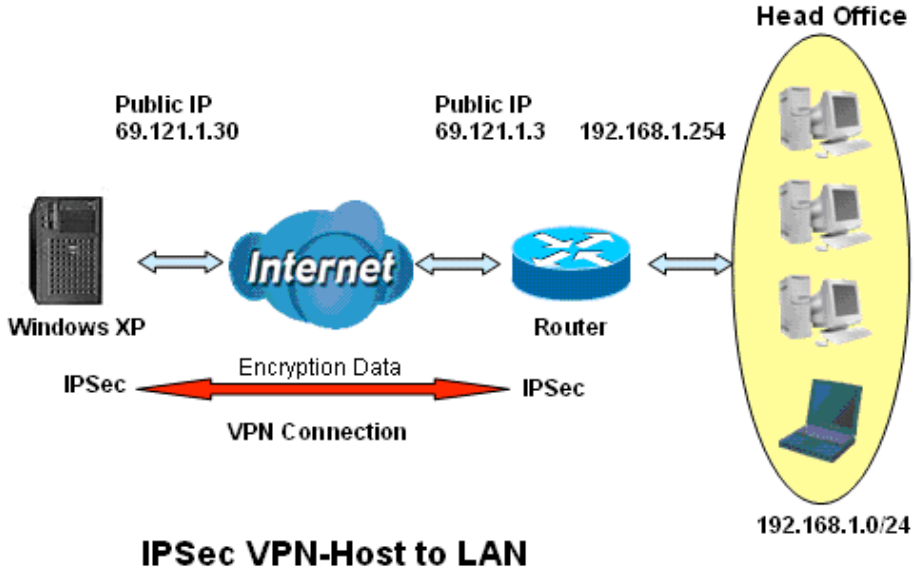
Item	Function		Description
1	Connection Name	IPSec_HeadOffice	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
4	Subnet		Check Subnet radio button
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	ESP		Check ESP radio button
	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

Configuring IPSec VPN in the Branch Office



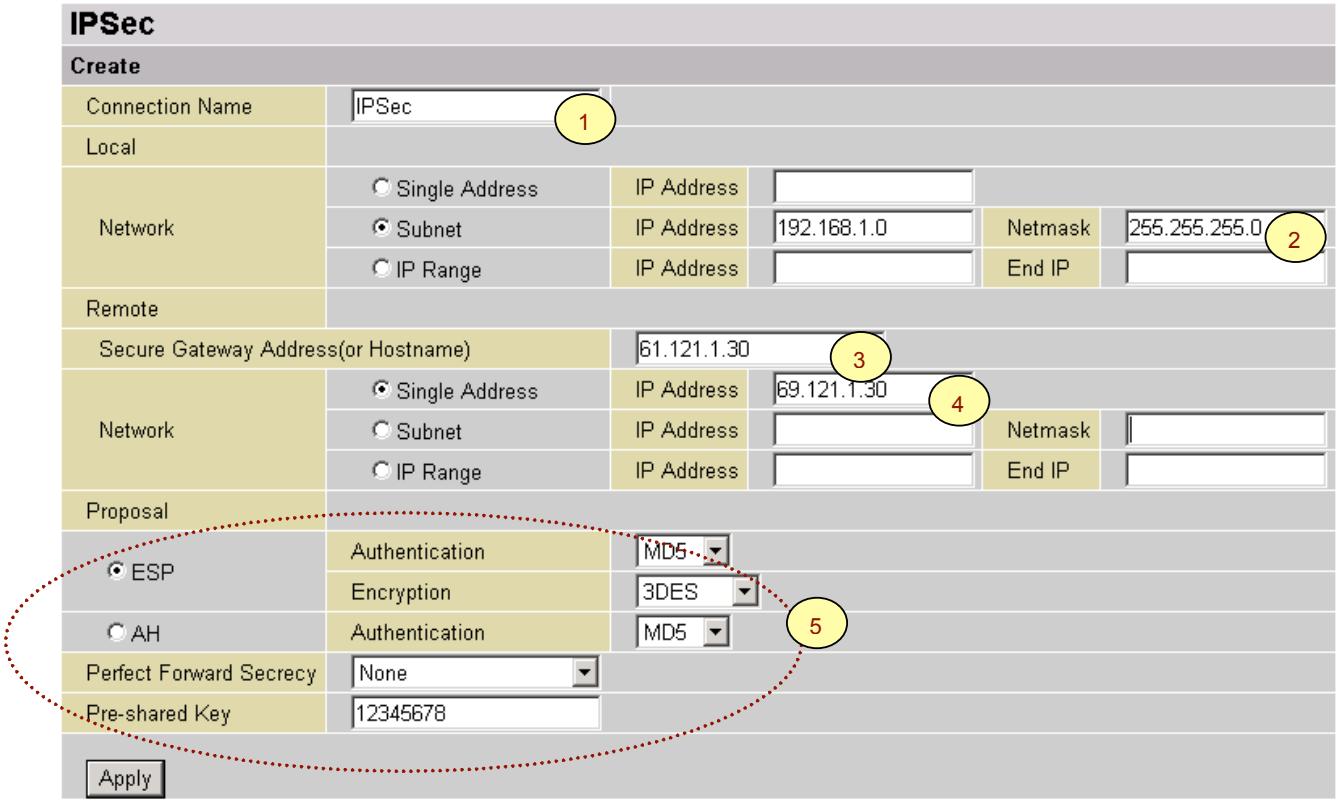
Item	Function		Description
1	Connection Name	IPSec_Branch Office	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.3	IP address of the head office router (in WAN side)
4	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	ESP		Check ESP radio button
	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

Example: Configuring a IPSec Host-to-LAN VPN Connection



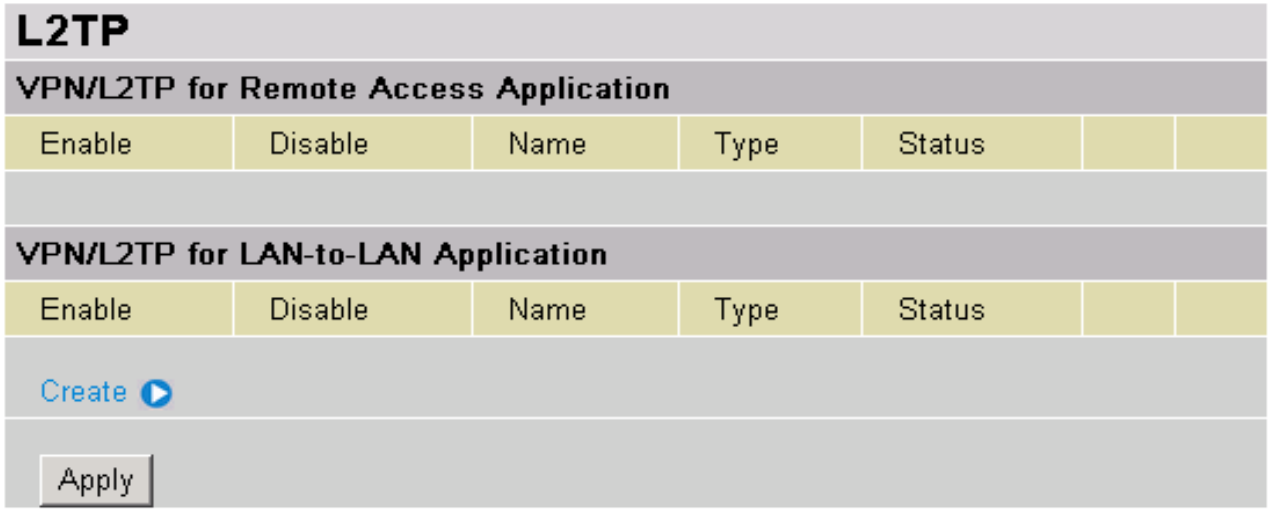
IPSec VPN-Host to LAN

Configuring IPSec VPN in the Office

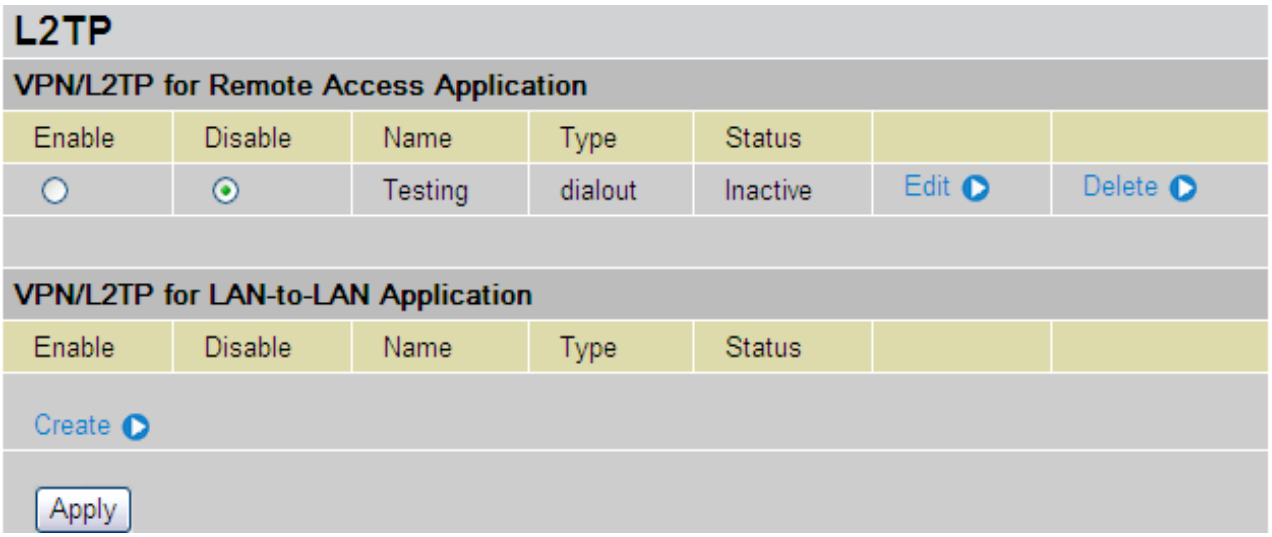


Item	Function		Description
1	Connection Name	IPSec	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
4	Single Address		Check Single Address radio button
	IP Address	69.121.1.30	Remote worker's IP address
5	ESP		Check ESP radio button
	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

L2TP (Layer Two Tunneling Protocol)



Two types of L2TP VPN are supported **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to create a new VPN connection account.



After you have created L2TP connection, account status will be displayed. (See example above).

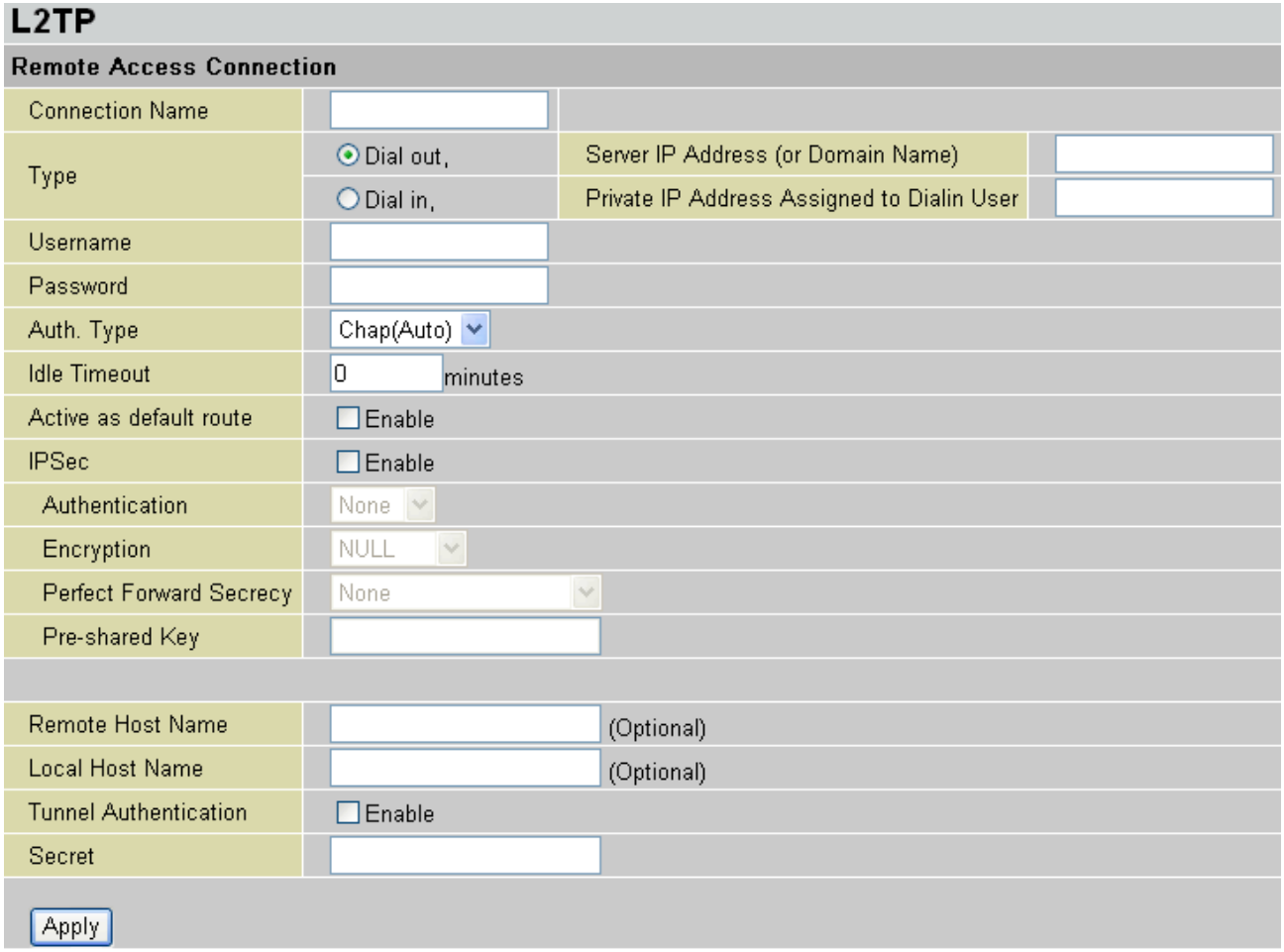
⊙ **Enable / Disable:** This function activates or deactivates the L2TP connection. To wish interrupting the tunnel, check **Disable** radio button and click **Apply** button to deactivate the connection.

Name: This is the user-defined name of the connection.

Type: This refers to your router operates as a client or a server, **Dialout** or **Dialin** in respectively.

Status: It informs your L2TP tunnel connection condition.

L2TP Connection - Remote Access



L2TP VPN Connection

Connection Name: User-defined name for the connection (e.g. “connection to office”).

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a pre-determined period of time. 0 means this connection is always on.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Click **Apply** after changing settings.

L2TP over IPSec (L2TP/IPSec) VPN Connection

IPSec: Enable for enhancing your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128_bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160_bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Remote Host Name (Optional): Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Cautious: This is only when the router performs as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. As default, Router's default Hostname is **home.gateway.**

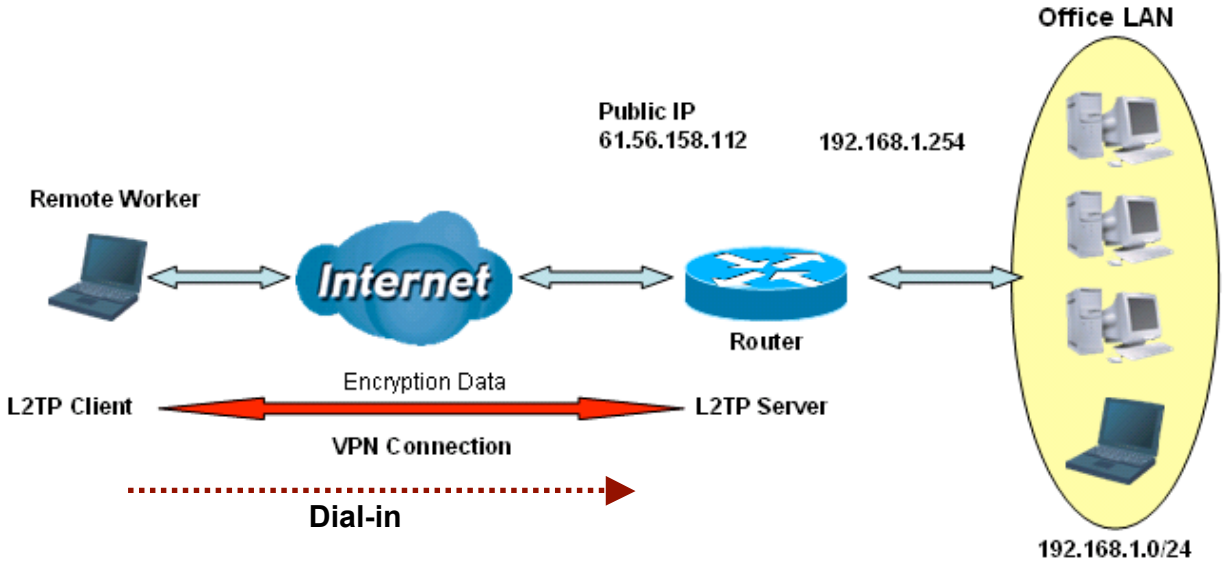
Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Click **Apply** after changing settings.

Example: Configuring a L2TP VPN - Remote Access Dial-in Connection

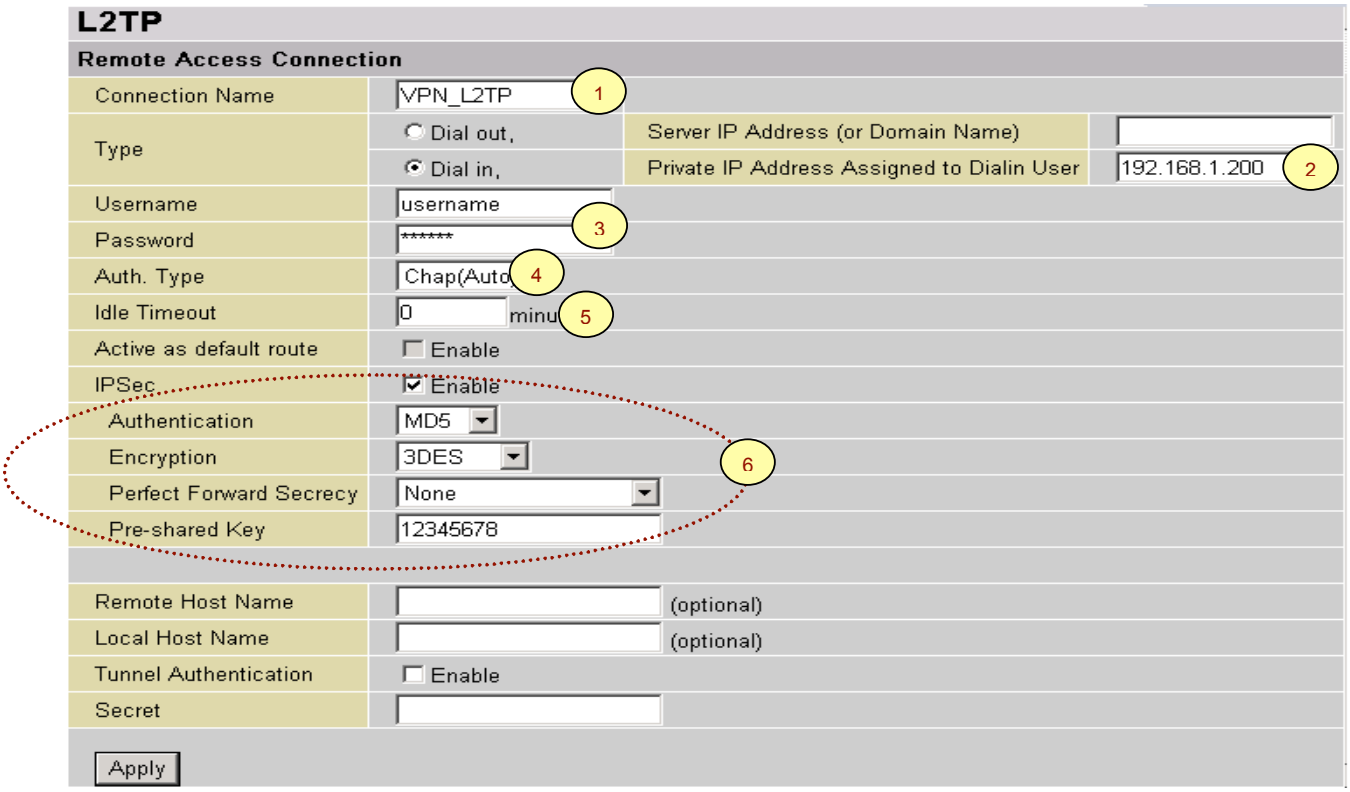
A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office, connected to a couple of PCs and Servers.



L2TP VPN-Remote Access (Dial-in)

Configuring L2TP VPN in the Office

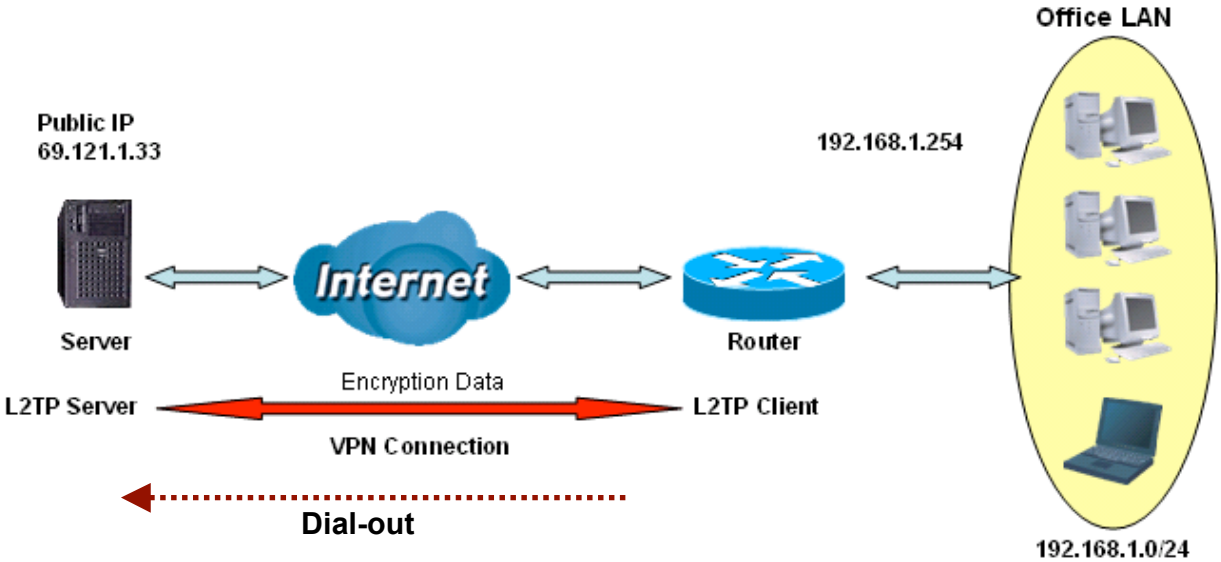
The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.



Item	Function		Description
1	Connection Name	VPN_L2TP	Given a name of L2TP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	An assigned IP address for the remote worker
3	Username	username	Input username & password to authenticate remote worker
	Password	123456	
4	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
5	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
6	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

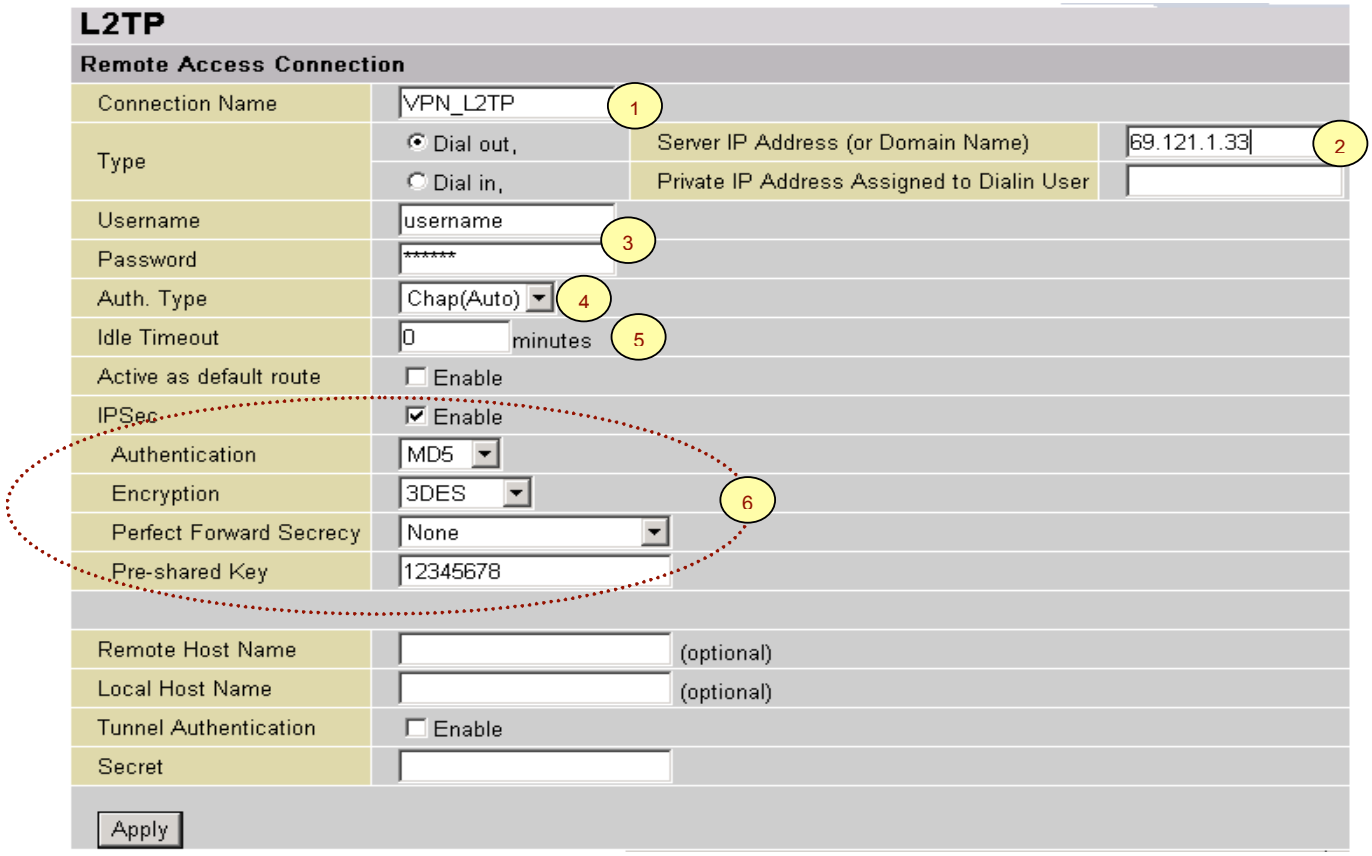
Example: Configuring a Remote Access L2TP VPN Dial-out Connection

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



L2TP VPN-Remote Access (Dial-out)

Configuring the L2TP VPN in the Office

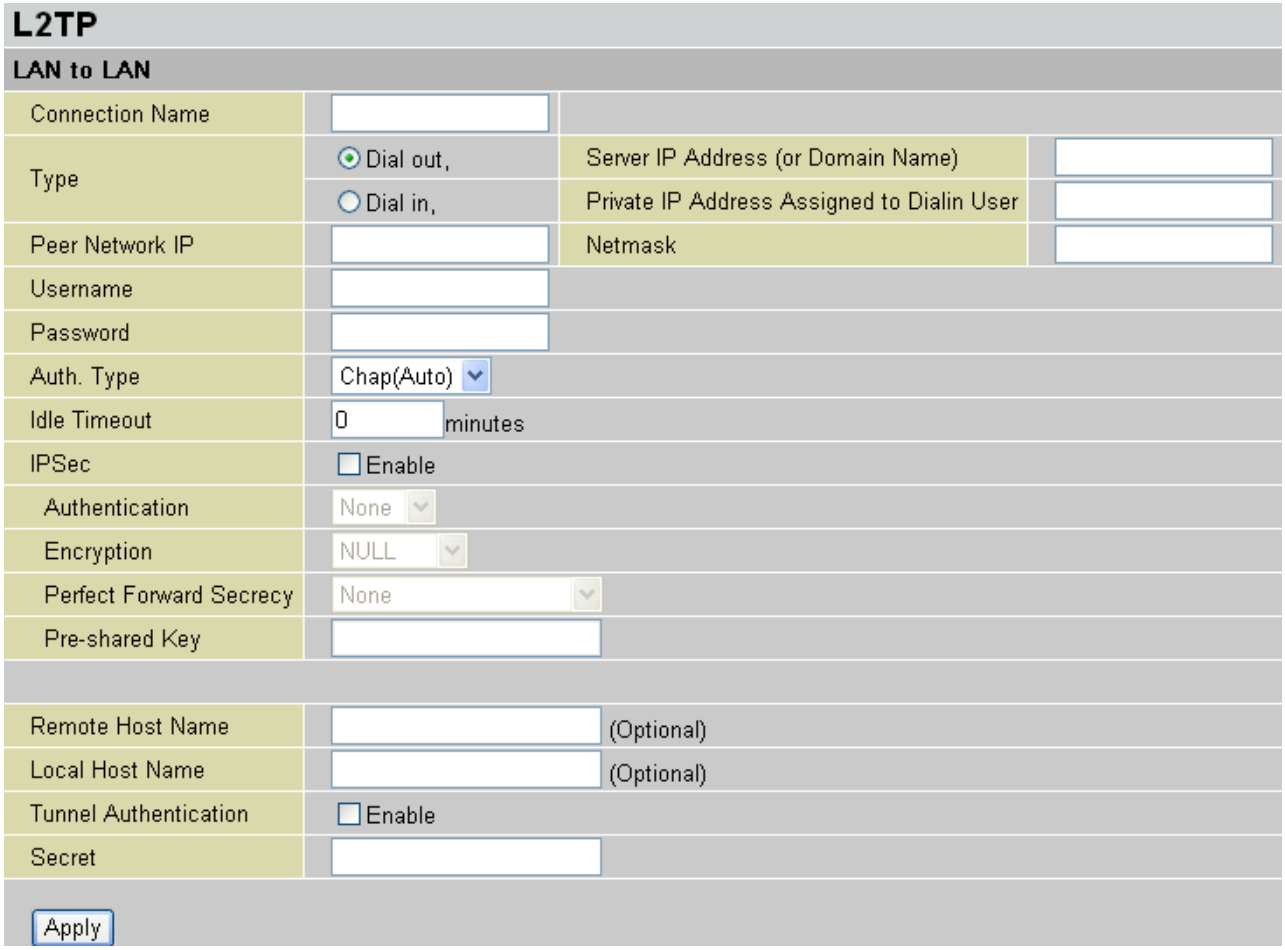


Item	Function		Description
1	Connection Name	VPN_L2TP	Given name of L2TP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	An Dialed server IP
3	Username	username	A given username & password
	Password	123456	
4	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
5	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
6	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring your Router to Dial-in to the Server

Currently, Microsoft Windows operation system does not support L2TP incoming service. Additional software may be required to set up your L2TP incoming service.

L2TP Connection - LAN to LAN



L2TP VPN Connection

Connection Name: User-define description of the connection.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router establish the connection to a remote LAN, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server to accept incoming connections, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by the your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after changing settings.

L2TP over IPSec (L2TP/IPSec) VPN Connection

IPSec: Enable for enhancing your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128_bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160_bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Remote Host Name (Optional): Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Cautious: This is only when the router performs as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. As default, Router's default Hostname is **home.gateway.**

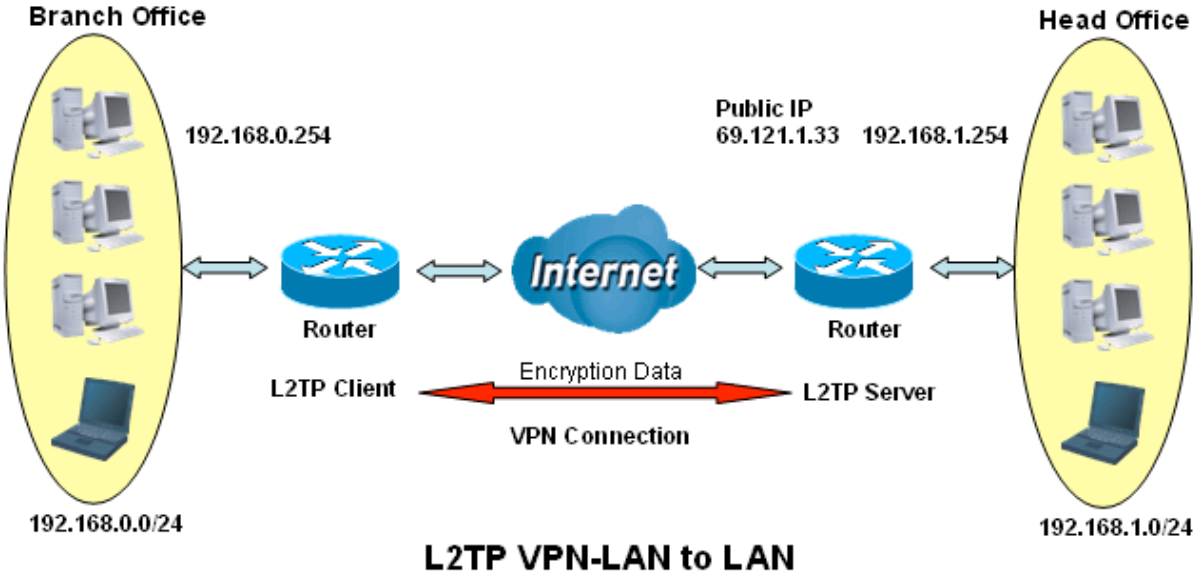
Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Click **Apply** after changing settings.

Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.



L2TP VPN-LAN to LAN

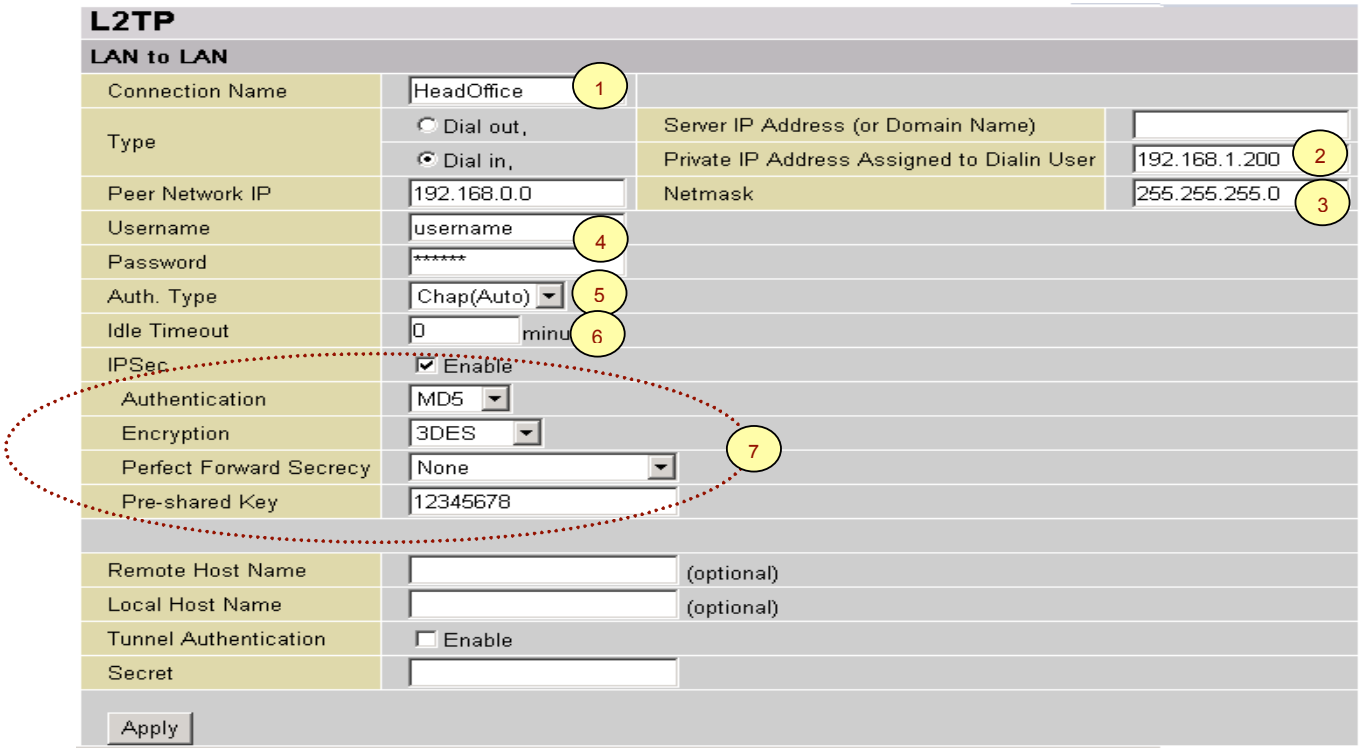
Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring L2TP VPN in the Head Office

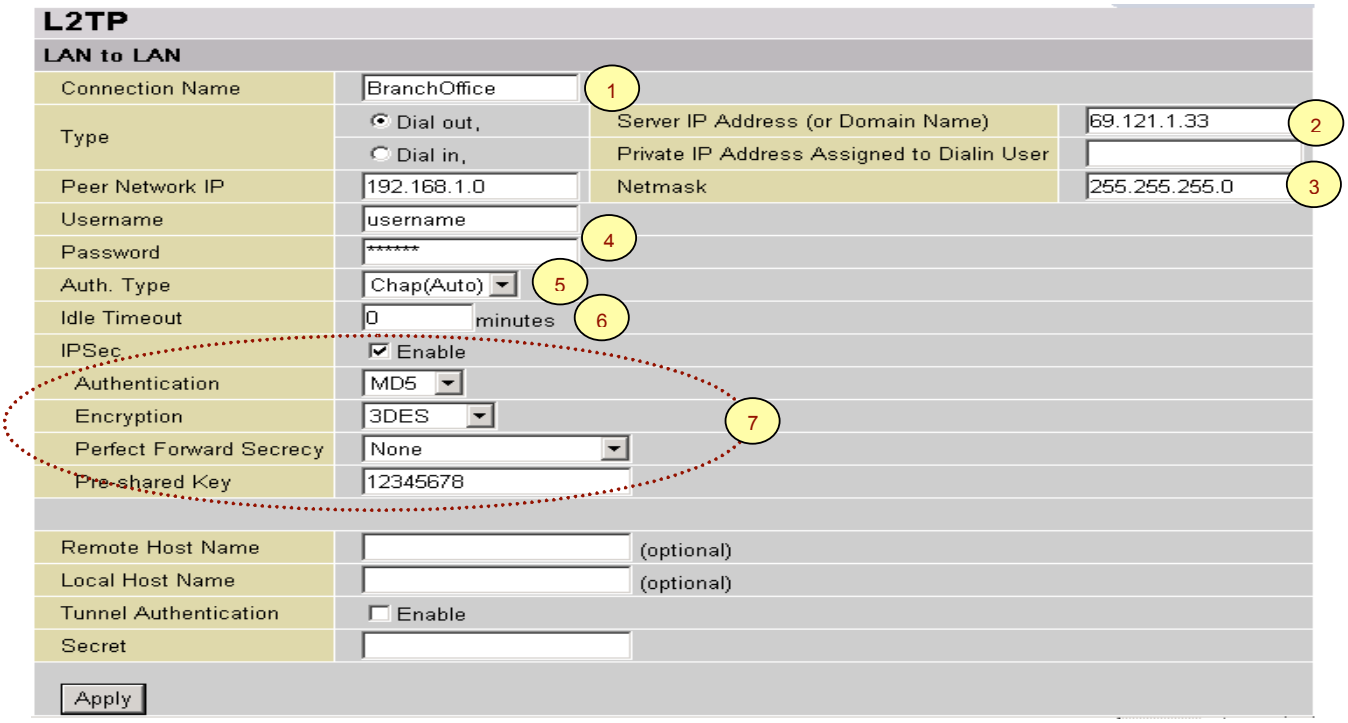
The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Connection Name	HeadOffice	Given a name of L2TP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	IP address assigned to branch office network
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
7	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Configuring L2TP VPN in the Branch Office

The IP address 69.1.121.30 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.



Item	Function		Description
1	Connection Name	BranchOffice	Given a name of L2TP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
7	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

QoS (Quality of Service)

QoS function helps you to control your network traffic for each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you to control the different quality and speed of through put for each application when the system is running with full loading of upstream.

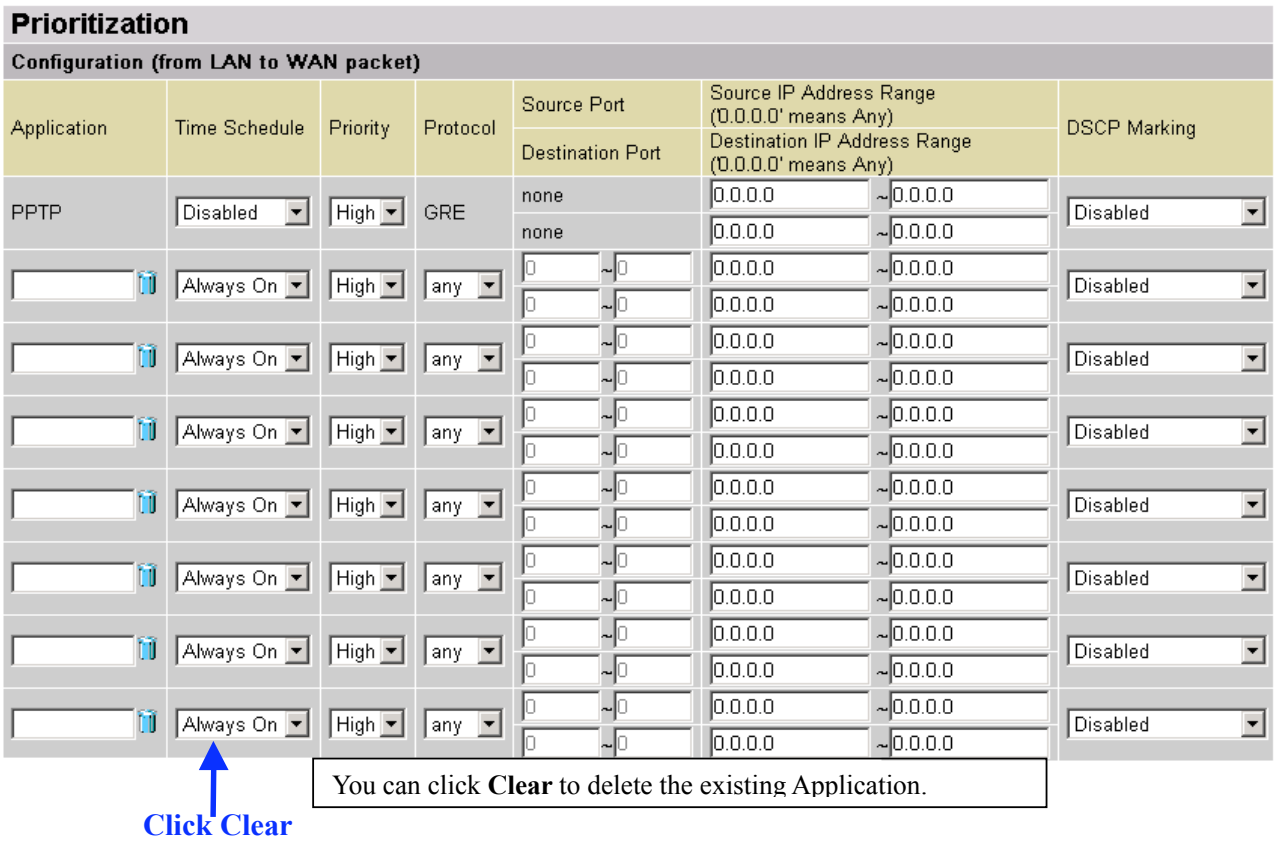
Here are items within the **QoS** section: **Prioritization** and **Outbound / Inbound IP Throttling** (bandwidth management).

Prioritization

There are three priority settings to be provided in the Router:

- **High**
- **Normal** (The default is normal priority for all of traffic without setting)
- **Low**

And the balances of utilization for each priority are High (60%), Normal (30%) and Low (10%).



Application: A user-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy.

Priority: The priority given to each policy/application. Its default setting is set to High; you may adjust this setting to fit your policy/application.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value. See Table 4. The DSCP Mapping Table:

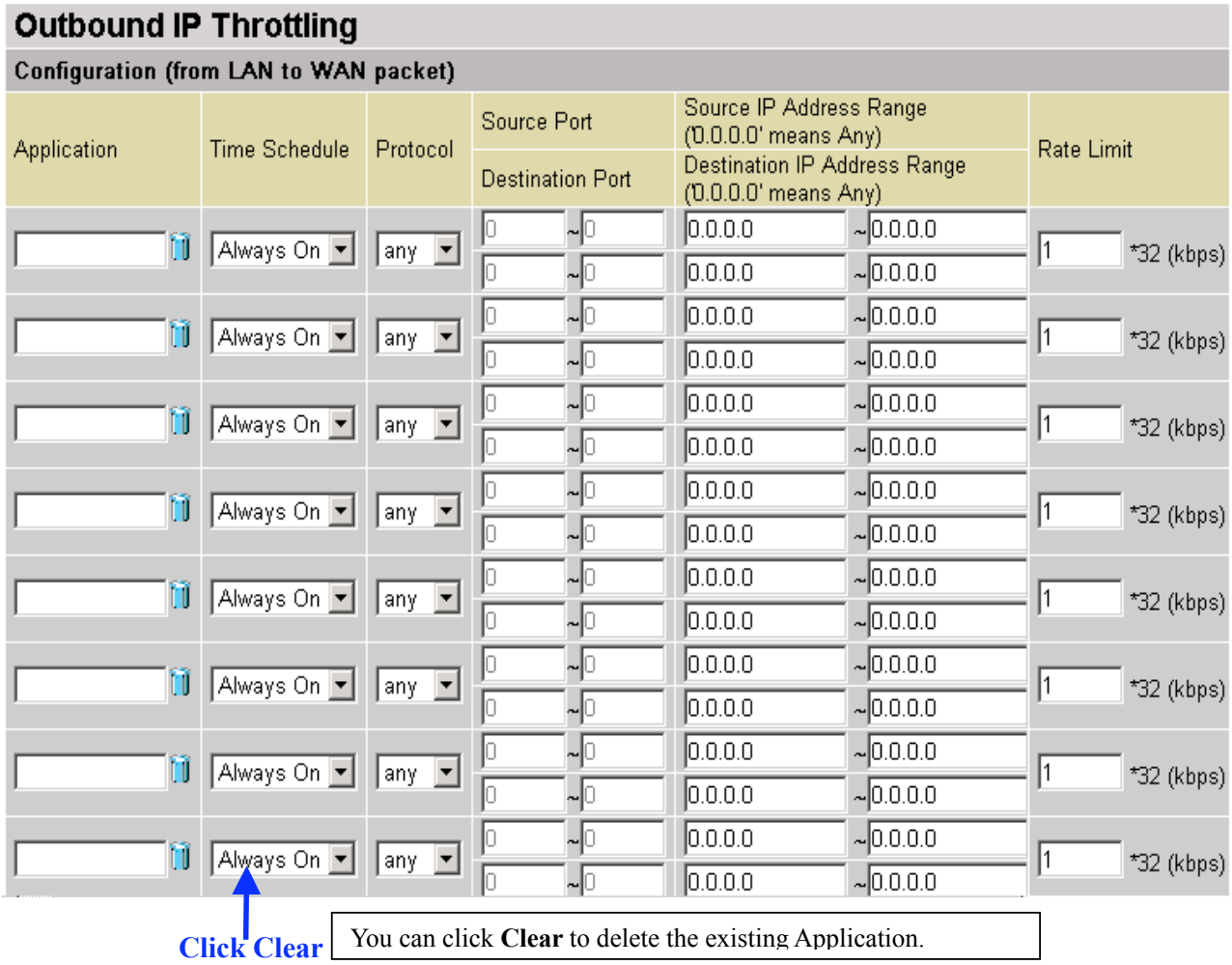
Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

Table 4: DSCP Mapping Table

DSCP Mapping Table	
SHDSL Router Device	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Outbound IP Throttling (LAN to WAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.



Application: A user-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

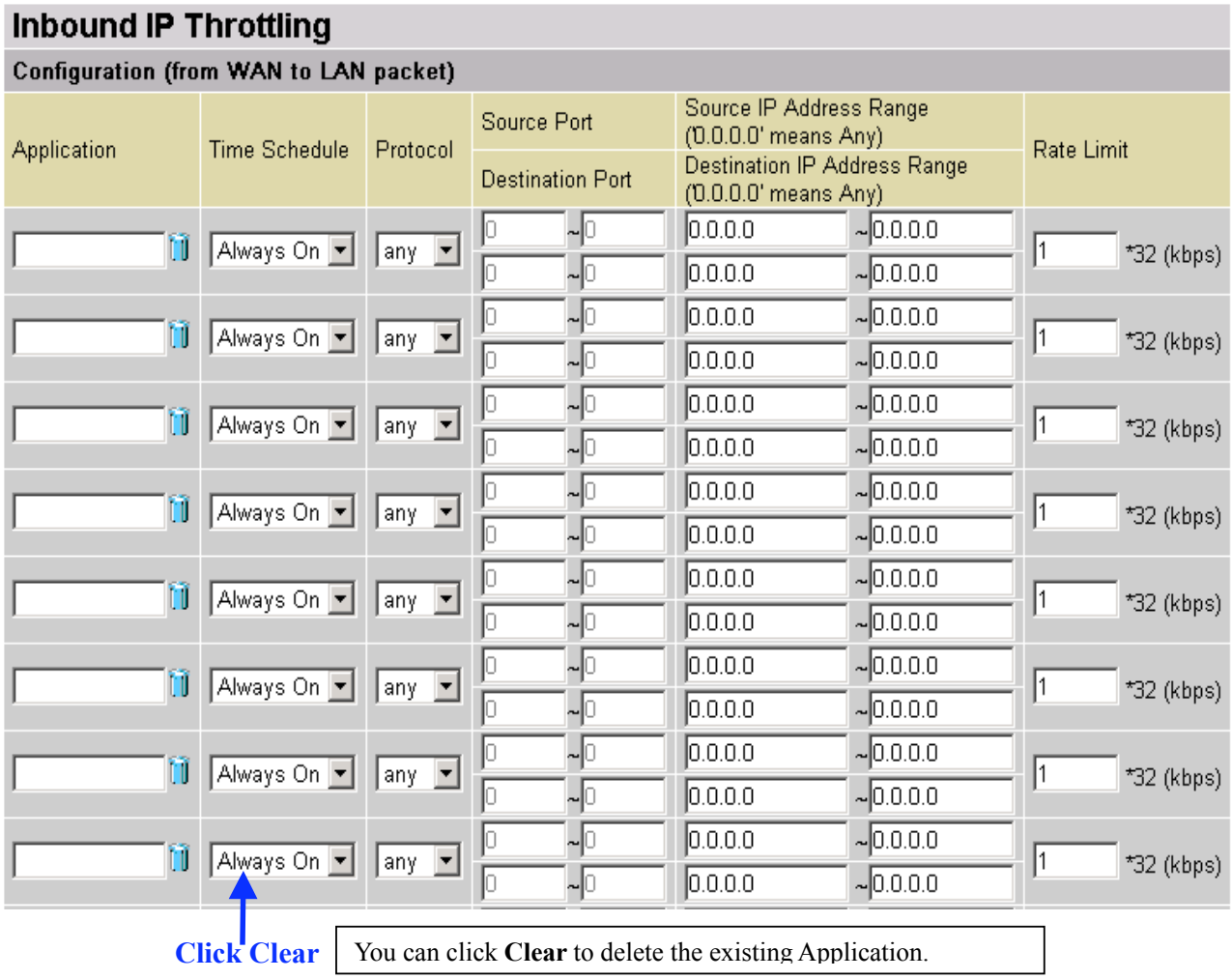
Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Outbound Rate Limit: To limit the speed of outbound traffic

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.



Application: A user-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

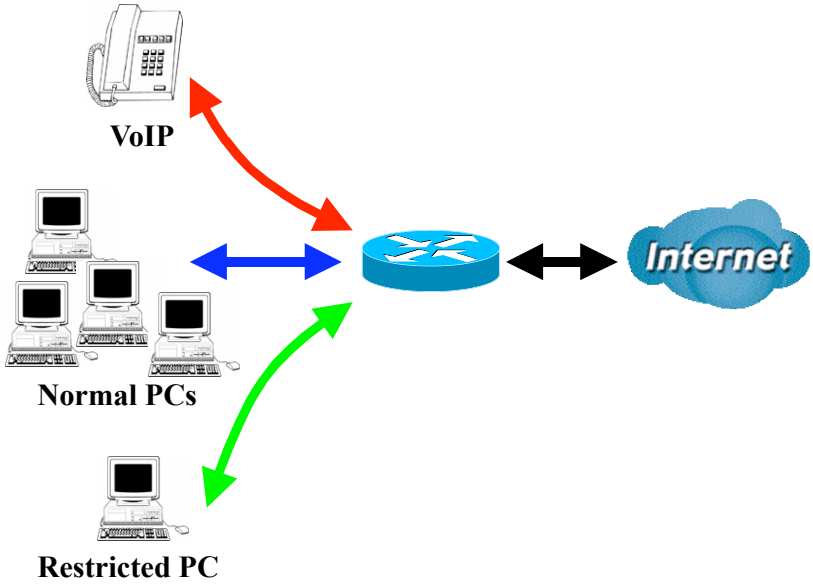
Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Inbound Rate Limit: To limit the speed of for inbound traffic.

Example: QoS for your Network

Connection Diagram



Information and Settings

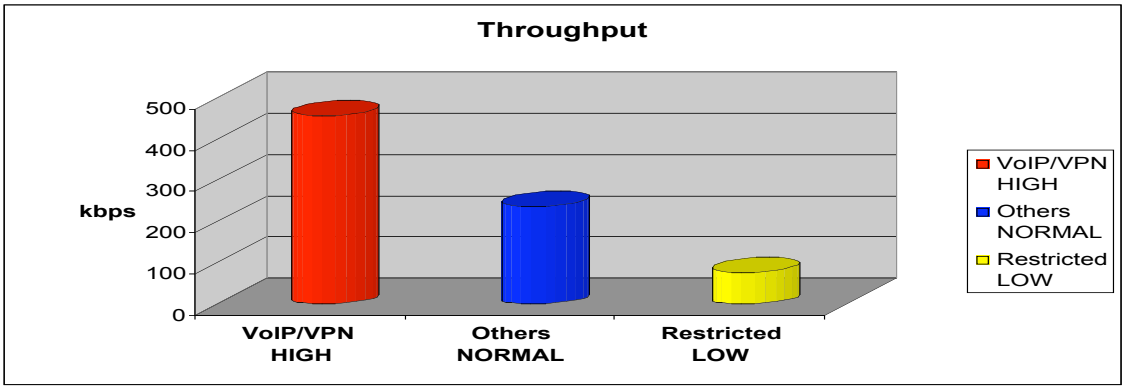
Upstream: 928 kbps
Downstream: 8 Mbps

VoIP User : 192.168.1.1
Normal Users : 192.168.1.2~192.168.1.5
Restricted User: 192.168.1.100

Prioritization

Configuration (from LAN to WAN packet)

Application	Time Schedule	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)	DSCP Marking
PPTP	Always On	High	GRE	none / none	0.0.0.0 ~ 0.0.0.0 / 0.0.0.0 ~ 0.0.0.0	Gold service (L)
VoIP	Always On	High	any	0 ~ 0 / 0 ~ 0	192.168.1.1 ~ 192.168.1.1 / 0.0.0.0 ~ 0.0.0.0	Gold service (L)
Restricted	TimeSlot1	Low	any	0 ~ 0 / 0 ~ 0	192.168.1.100 ~ 192.168.1.100 / 0.0.0.0 ~ 0.0.0.0	Gold service (L)



Mission-critical application

Mostly the VPN connection is mission-critical application for doing data exchange between head and branch office.

PPTP	Always On	High	GRE	none	0.0.0.0 ~ 0.0.0.0	Gold service (L)
				none	0.0.0.0 ~ 0.0.0.0	

The mission-critical application must be sent out smoothly without any dropping. Set priority as high level for preventing any other applications to saturate the bandwidth.

Voice application

Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

VoIP	Always On	High	any	0 ~ 0	192.168.1.1 ~ 192.168.1.1	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	

Above settings will help to improve quality of your VoIP service when traffic is full loading.

Restricted Application

Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.

Restricted	TimeSlot1	Low	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	

With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at daytime.

Advanced setting by using IP throttling

With IP throttling you can specify more detail for allocating bandwidth; even the applications are located in the same level.

Upstream: 928kbps (29*32kbps)
Mission-critical Application: 192kbps (6*32kbps)
Voice Application: 128kbps (4*32kbps)
Restricted Application: 160kbps (5*32kbps)
Other Applications: 448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Application	Time Schedule	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)	Rate Limit
PPTP	Always On	gre	0 ~ 0 / 0 ~ 0	0.0.0.0 ~ 0.0.0.0 / 0.0.0.0 ~ 0.0.0.0	6 *32 (kbps)
VoIP	Always On	any	0 ~ 0 / 0 ~ 0	0.0.0.0 ~ 0.0.0.0 / 0.0.0.0 ~ 0.0.0.0	4 *32 (kbps)
Restricted	TimeSlot1	any	0 ~ 0 / 0 ~ 0	192.168.1.100 ~ 192.168.1.100 / 0.0.0.0 ~ 0.0.0.0	5 *32 (kbps)
Others	TimeSlot1	any	0 ~ 0 / 0 ~ 0	192.168.1.2 ~ 192.168.1.5 / 0.0.0.0 ~ 0.0.0.0	14 *32 (kbps)

Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below help you to limit bandwidth for the restricted application.

Inbound IP Throttling

Configuration (from WAN to LAN packet)

Application	Time Schedule	Protocol	Source Port Destination Port	Source IP Address Range ('0.0.0.0' means Any) Destination IP Address Range ('0.0.0.0' means Any)	Rate Limit
Restricted	TimeSlot1	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 192.168.1.100 ~ 192.168.1.100	64 *32 (kbps)

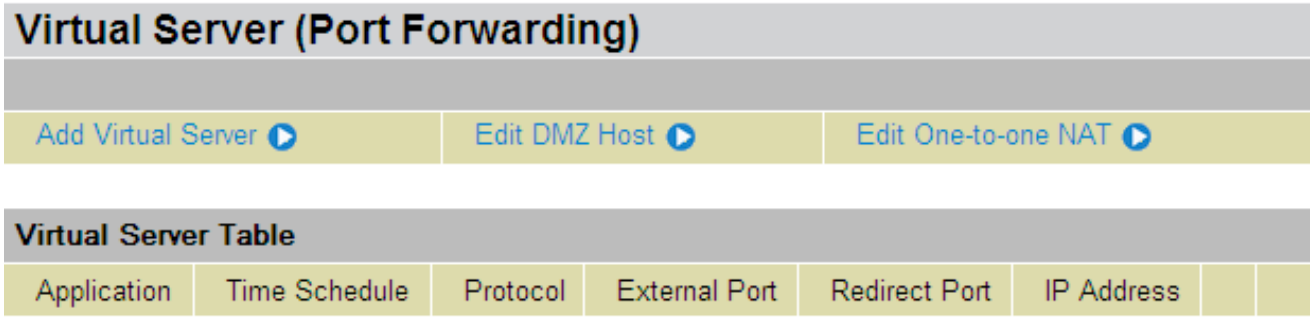
Virtual Server ("Port Forwarding")

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

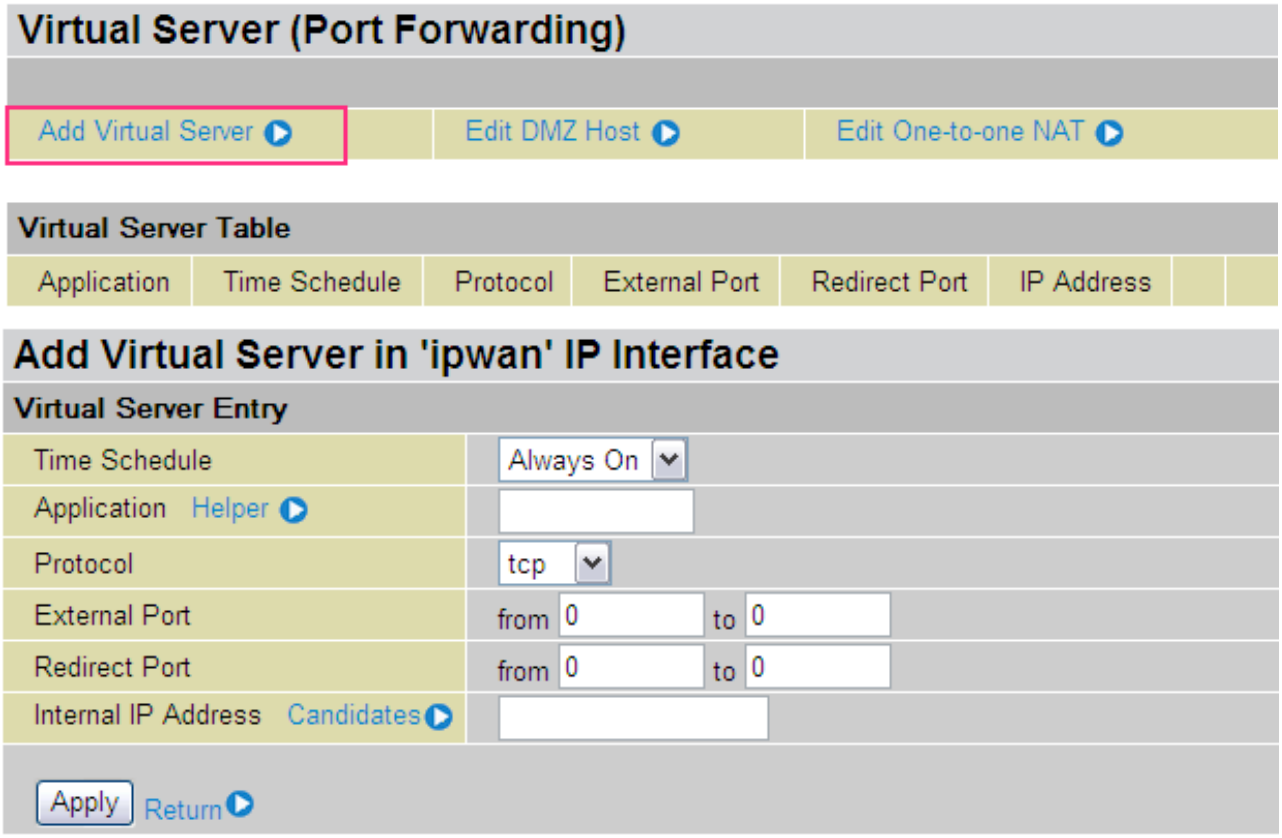
The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network



Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.



Time Schedule: A self-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

Application: Users-define description to identify this entry or click Helper to select existing predefined rules.

Helper **:** 20 predefined rules are available. Click the Radio button to select the rule; Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

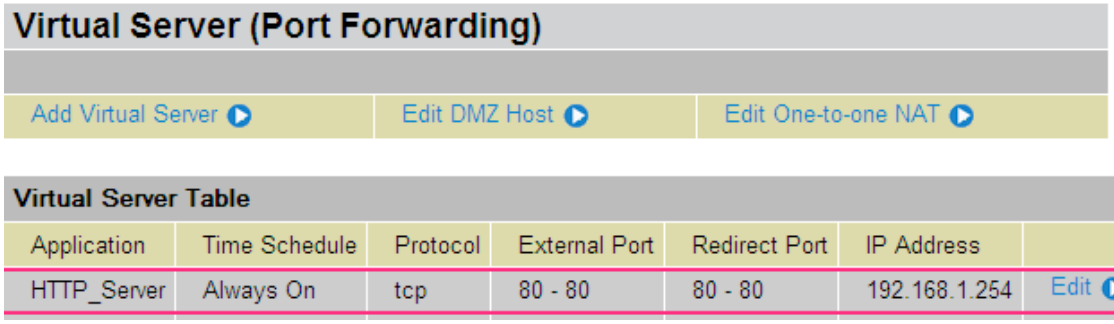
Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application.

Candidates List all existing PCs connecting to the network. Y ou may assign a PC with IP address and MAC from this list.

Example:

If you like to remote accessing your Router through the Web/HTTP at all time, you would need to enable port number 80 (Web/HTTP) and map to Router's IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the **Application** click **Helper.** A list of predefined rules window will pop and select **HTTP_Sever**.

Application: *HTTP_Sever*
Time Schedule: *Always On*
Protocol: *tcp*
External Port: *80-80*
Redirect Port: *80-80*
IP Address: *192.168.1.254*



Edit: Click it to edit this virtual server application.

Delete: Click it to delete this virtual server application.

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention

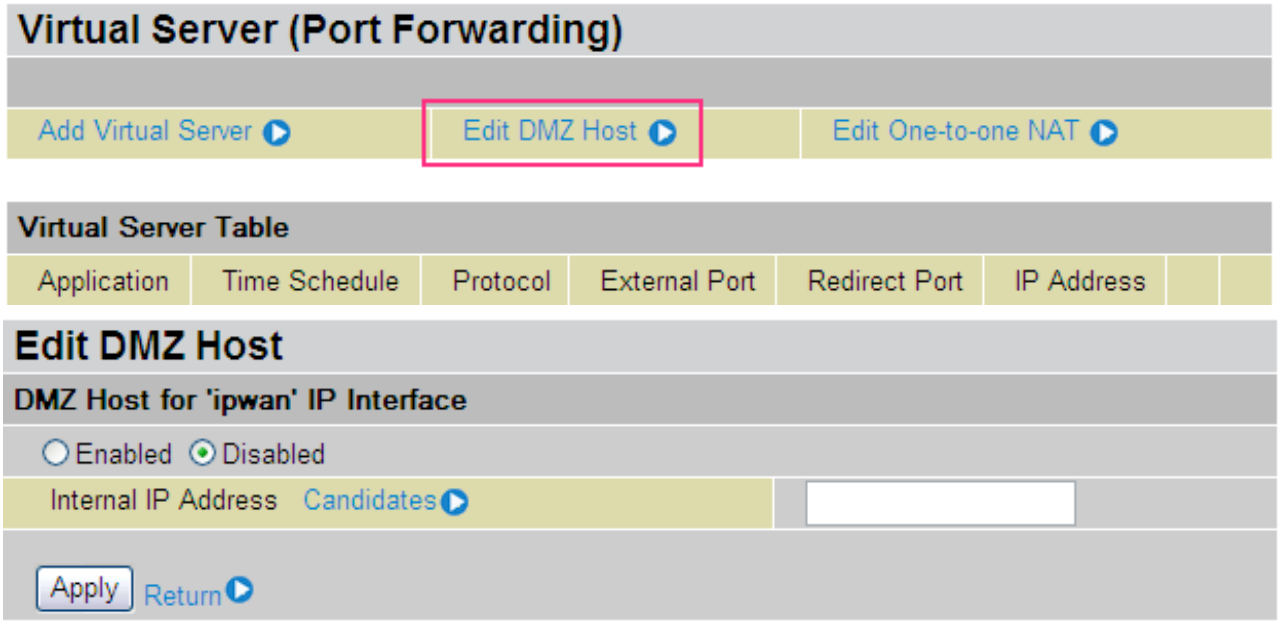
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Edit DMZ Host

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

Cautious: This Local computer exposing to the Internet may face varies of security risks.



- **Disabled:** As set in default setting, it disables the DMZ function.
- **Enabled:** It activates your DMZ function.

Internal IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

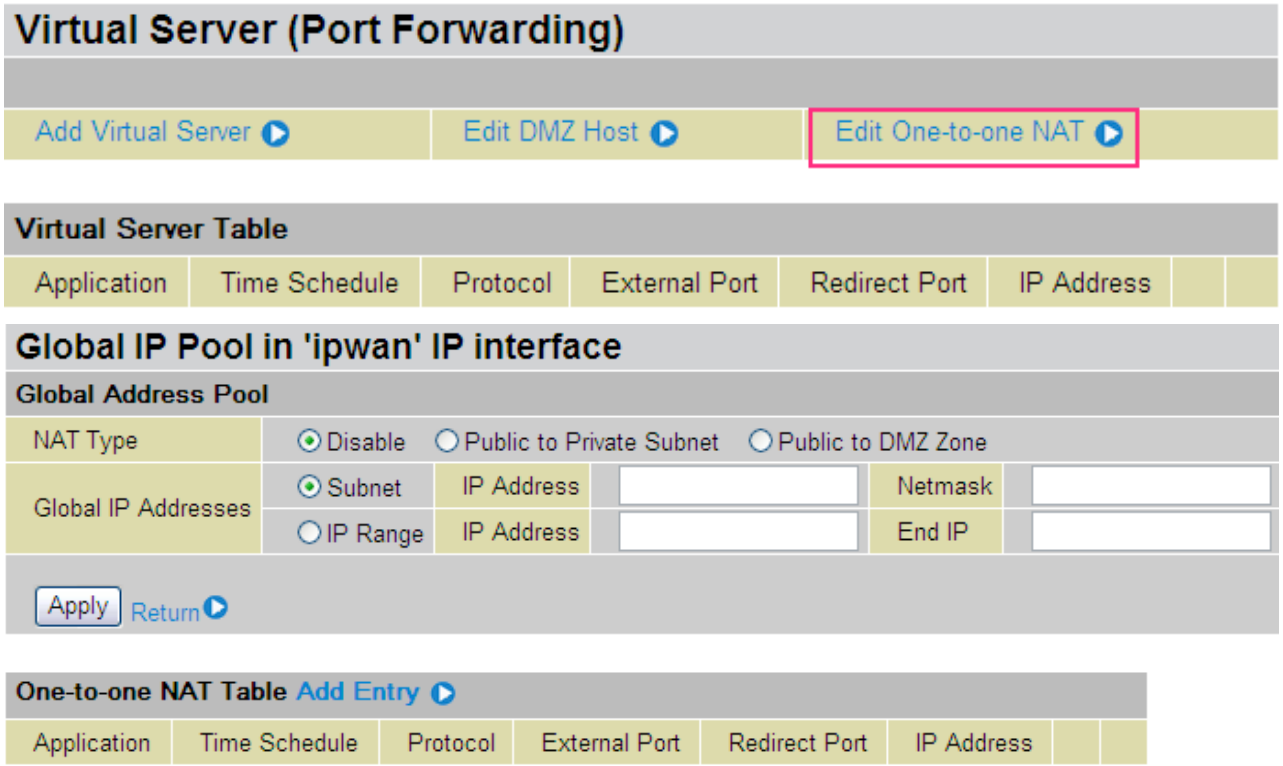
Candidates List all the connecting PCs on the network. You may assign specific PC with its IP address and MAC from the list.

Select the **Apply** button to apply your changes.

Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private/local IP address to a global/public IP address.

If you have multiple public/WAN IP addresses from you ISP, you are eligible for One-to-One NAT to utilize these IP addresses.



NAT Type: Select desired NAT type. As set in default setting, it disables the One-to-One NAT function.

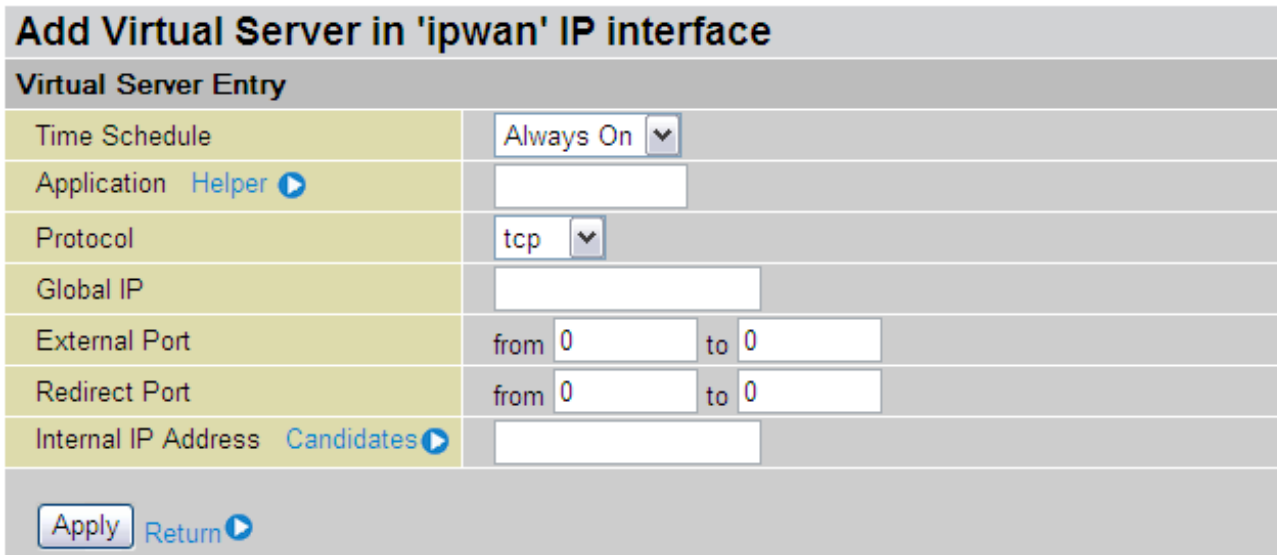
Global IP Address:

⊙ **Subnet:** The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.

⊙ **IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Select the **Apply** button to apply your changes.

Check Add Entry to create a new One-to-One NAT rule:



Time Schedule: A self-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

Application: Users-defined description to identify this entry or click Helper to select existing predefined rules.

Helper **:** 20 predefined rules are available. Click the Radio button to select the rule; Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP;

Global IP: Define a public/ WAN IP address for this Application to use. This Global IP address must be defined in the **Global IP Address.**

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application.

Candidates List all the connecting PCs on the network. You may assign specific PC with its IP address and MAC from the list.

Select the **Apply** button to apply your changes.

Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

For further information, please see IANA’s website at: http://www.iana.org/assignments/port-numbers

Table 5: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Time Schedule

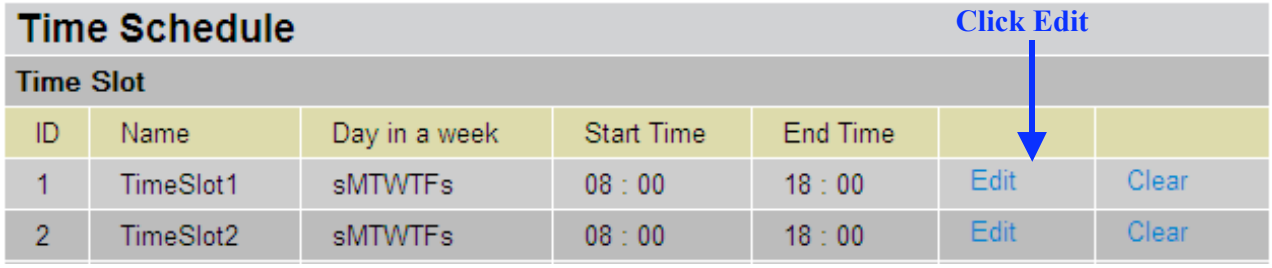
Time Slot

ID	Name	Day in a week	Start Time	End Time		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Edit	Clear
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Edit	Clear
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Edit	Clear
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Edit	Clear
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Edit	Clear
6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	Edit	Clear
7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	Edit	Clear
8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	Edit	Clear
9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	Edit	Clear
10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	Edit	Clear
11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	Edit	Clear
12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	Edit	Clear
13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	Edit	Clear
14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	Edit	Clear
15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	Edit	Clear
16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	Edit	Clear

Configuration of Time Schedule

Edit a Time Slot

1. Choose any Time Slot (ID 1 to ID 16) to edit, click **Edit.**



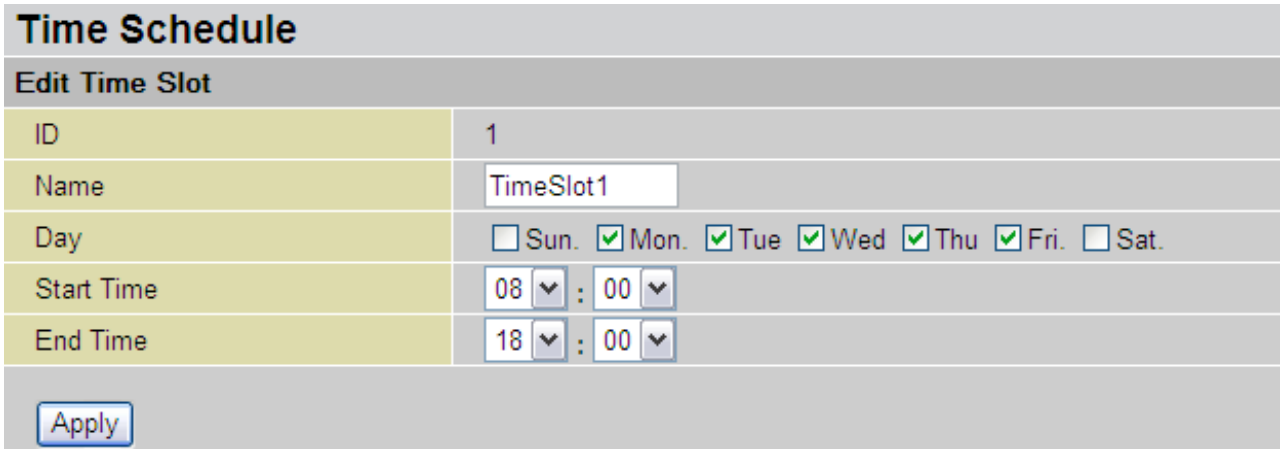
Time Schedule

Time Slot

ID	Name	Day in a week	Start Time	End Time		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Edit	Clear
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Edit	Clear

Note: Watch it carefully, the days you have selected will present in capital letter. Lower case letter shows the day(s) is not selected, and no rule will apply on this day(s).

2. A detailed setting of this Time Slot will be shown.



Time Schedule

Edit Time Slot

ID	1
Name	TimeSlot1
Day	☐ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. ☐ Sat.
Start Time	08 : 00
End Time	18 : 00

Apply

ID: This is the index of the time slot.

Name: A user-define description to identify this time portfolio.

Day: The default is set from Monday through Friday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

Select the **Apply** button to apply your changes.

Delete a Time Slot

Click **Clear** to delete the existing Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

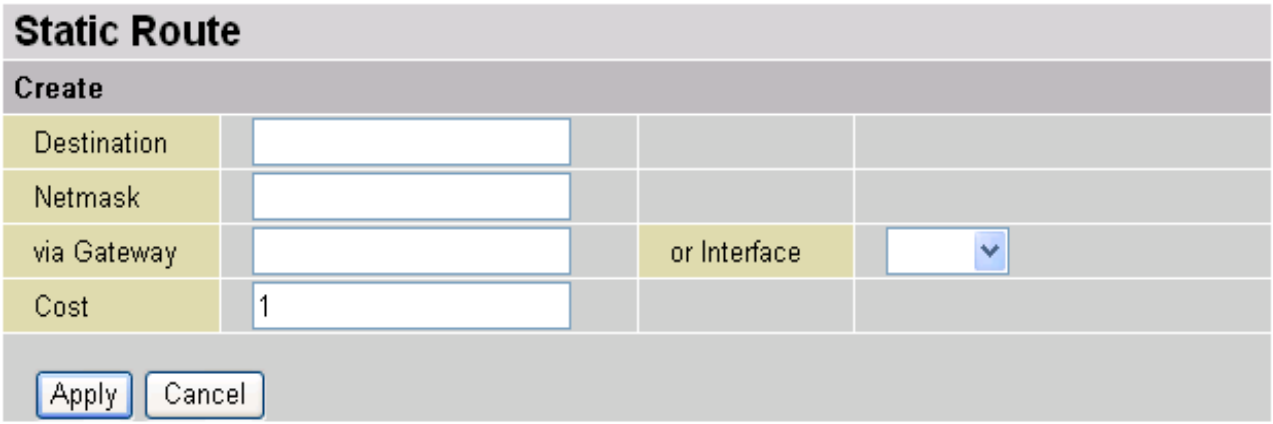
Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are items within the **Advanced** section: **Static Route, Dynamic DNS, Check Email, Device Management, IGMP and VLAN Bridge.**

Static Route

Click on **Routing Table** and then choose **Create Route** add a routing table.



Destination: This is the destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses based on above destination subnet IP.

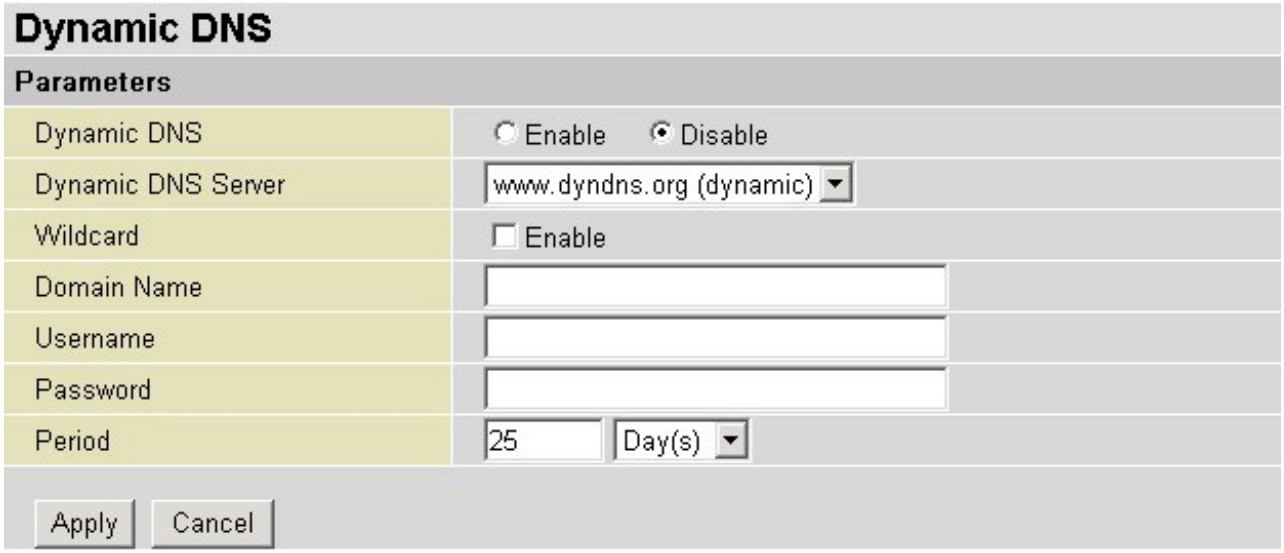
Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your SHDSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/

There are more than 5 DDNS services supported.

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The following fields will be activated and required:

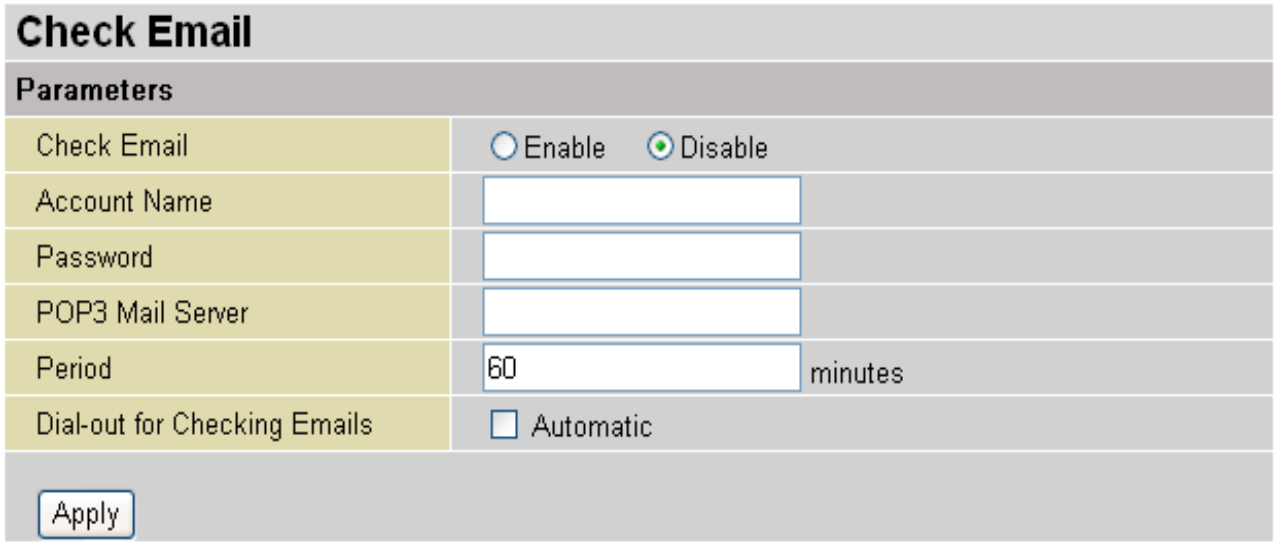
Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Check Email

This function allows you to have the router check your POP3 mailbox for new Email messages. The Mail LED on your router will light when it detects new messages waiting for download. You may also view the status of this function using the Status – Email Checking section of the web interface, which also provides details on the number of new messages waiting. See the Status section of this manual for more information.



⊙ **Disable:** Check to disable the router's Email checking function.

⊙ **Enable:** Check to enable the routers Email checking function. The following fields will be activated and required:

Account Name: Enter the name (login) of the POP3 account you wish to check.. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account's password.

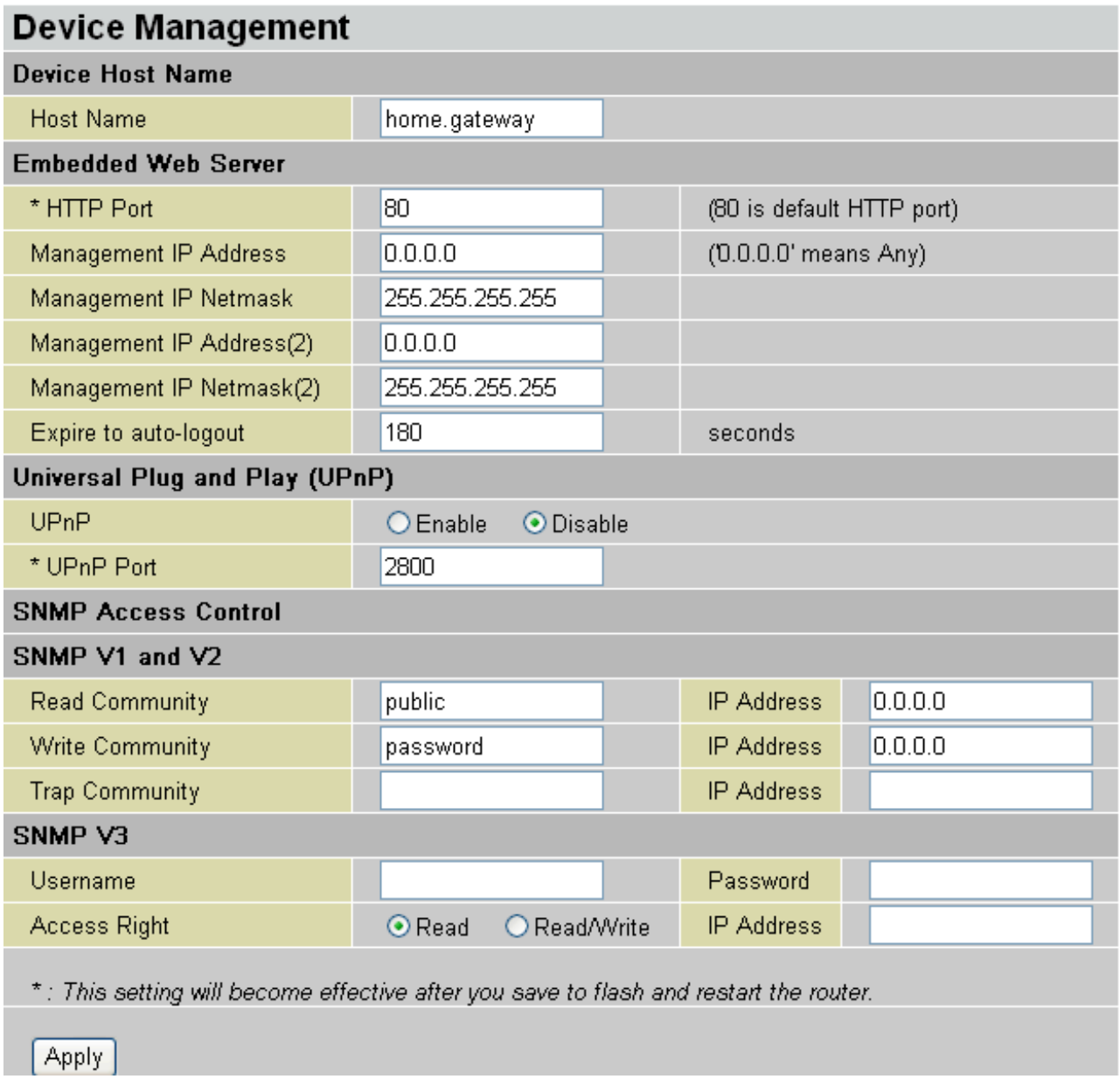
POP3 Mail Server: Enter your (POP) mail server name. You Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Period: Enter the value in minutes between periodic mail checks.

Automatically dial-out for checking emails: When the function is enabled, your router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your SHDSL service is charged by time online.

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Device Management

Device Host Name			
Host Name	home.gateway		
Embedded Web Server			
* HTTP Port	80	(80 is default HTTP port)	
Management IP Address	0.0.0.0	('0.0.0.0' means Any)	
Management IP Netmask	255.255.255.255		
Management IP Address(2)	0.0.0.0		
Management IP Netmask(2)	255.255.255.255		
Expire to auto-logout	180	seconds	
Universal Plug and Play (UPnP)			
UPnP	○ Enable ◉ Disable		
* UPnP Port	2800		
SNMP Access Control			
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	◉ Read ○ Read/Write	IP Address	

** : This setting will become effective after you save to flash and restart the router.*

Apply

Embedded Web Server (2 Management IP accounts)

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** seconds. The router will only allow User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: http://**192.168.1.254:100** in their web browser. After 100 seconds, the device will automatically logout User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

- ⊙ **Disable:** Check to disable the router's UPnP functionality.
- ⊙ **Enable:** Check to enable the router's UPnP functionality.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used you may wish to change the port.

SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

- ☑ System group
- ☑ Interfaces group
- ☑ Address Translation group
- ☑ IP group
- ☑ ICMP group
- ☑ TCP group
- ☑ UDP group
- ☒ EGP (not applicable)
- ☑ Transmission

☑ SNMP group

From RFC1650 (EtherLike-MIB):

☑ dot3Stats

From RFC 1493 (Bridge MIB):

☑ dot1dBase group

☑ dot1dTp group

☑ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

☑ pppLink group

☒ pppLqr group (not applicable)

From RFC 1472 (PPP/Security MIB):

☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

☑ PPP Bridge Group

From RFC1573 (IfMIB):

☑ ifMIBObjects Group

From RFC1695 (atmMIB):

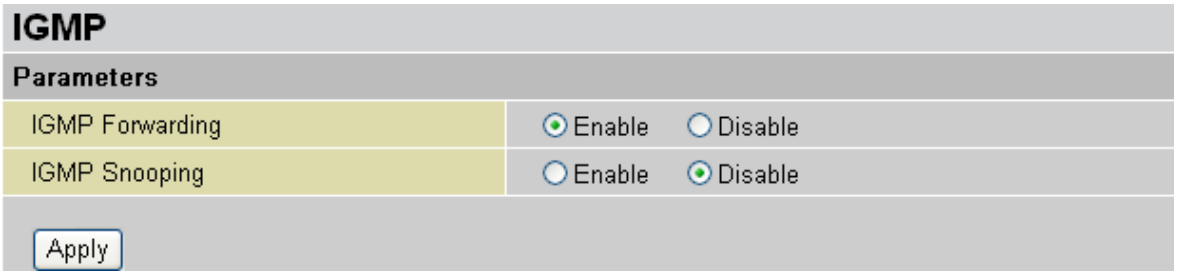
☑ atmMIBObjects

From RFC 1907 (SNMPv2):

☑ only snmpSetSerialNo OID

IGMP

IGMP, known as *Internet Group Management Protocol*, is used to management hosts from multicast group.

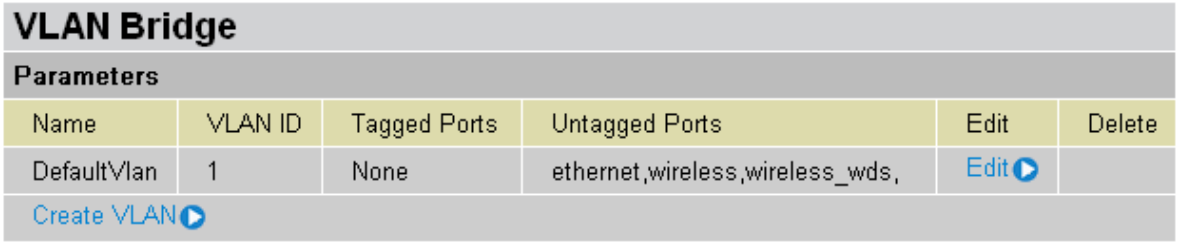


IGMP Forwarding: Accepting multicast packet. Default is set to **Enable.**

IGMP Snooping: Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to **Disable.**

VLAN Bridge

This section allows you to create VLAN group and specify the member.



Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Advanced VLAN Setup Example (Triply Play)

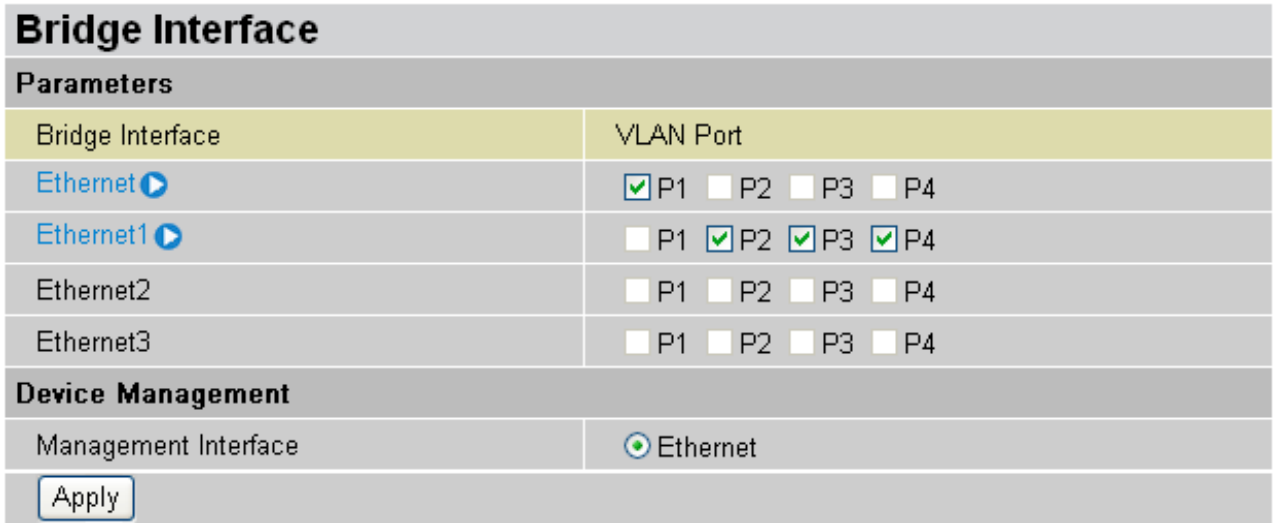
VLAN_data:
Ethernet Port 1, Wireless and Wireless_WDS are reserving for Internet
- On Ethernet port 1 I also need VC 0/40 bridged.

VLAN_Vedio
Ethernet ports: 2, 3 and 4:
- 0/33 Bi-directional IP
- 0/34 Video
- 0/35 Video
- 0/36 Video Subscriber Services (EPG, EAS, etc.)
- 0/37 Video
- 0/38 Video
- 0/39 Spare

Step 1: Setup Member Ports

Go to **Configuration → LAN → Bridge Interface.**
You can setup member ports for each VLAN group under Bridge Interface section. From the example, two VLAN groups need to be created.
Ethernet: P1 (Port 1)
Ethernet1: P2, P3 and P4 (Port 2, 3, 4) Please uncheck P2, P3, P4 from Ethernet VLAN Port first.
Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4



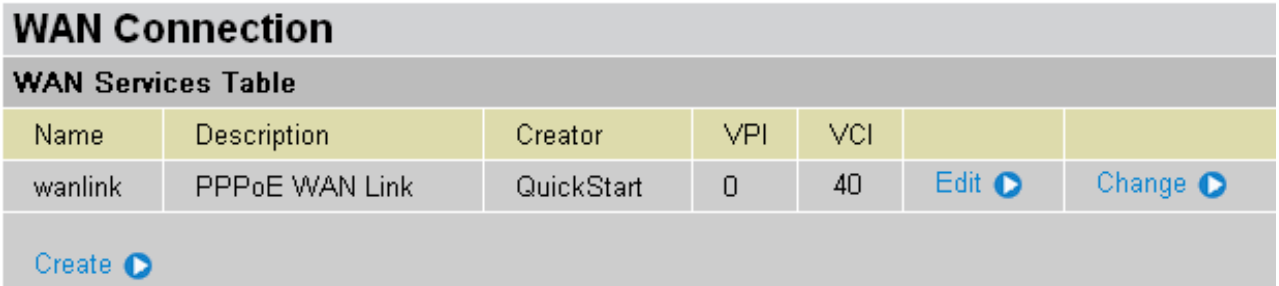
Step 2: Create WAN Interface

Go to **Configuration → WAN→ ISP**

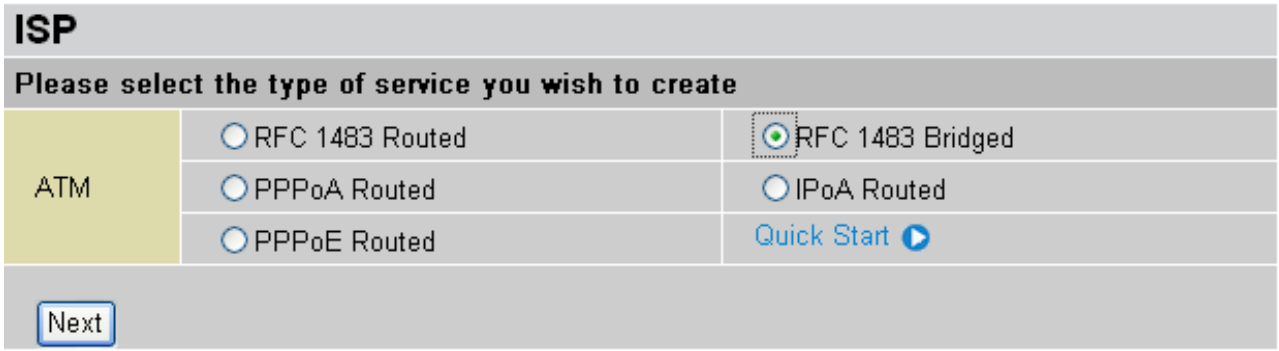
wanlink is the factory default WAN interface which in service for data/internet access. If your ISP uses this access protocol, click **Edit** to input other parameters if needed. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

From the example, 0/40 is used for data/internet and assumes PPPoE is used; click the **Edit** to change the VPI/VCI to 0/40.

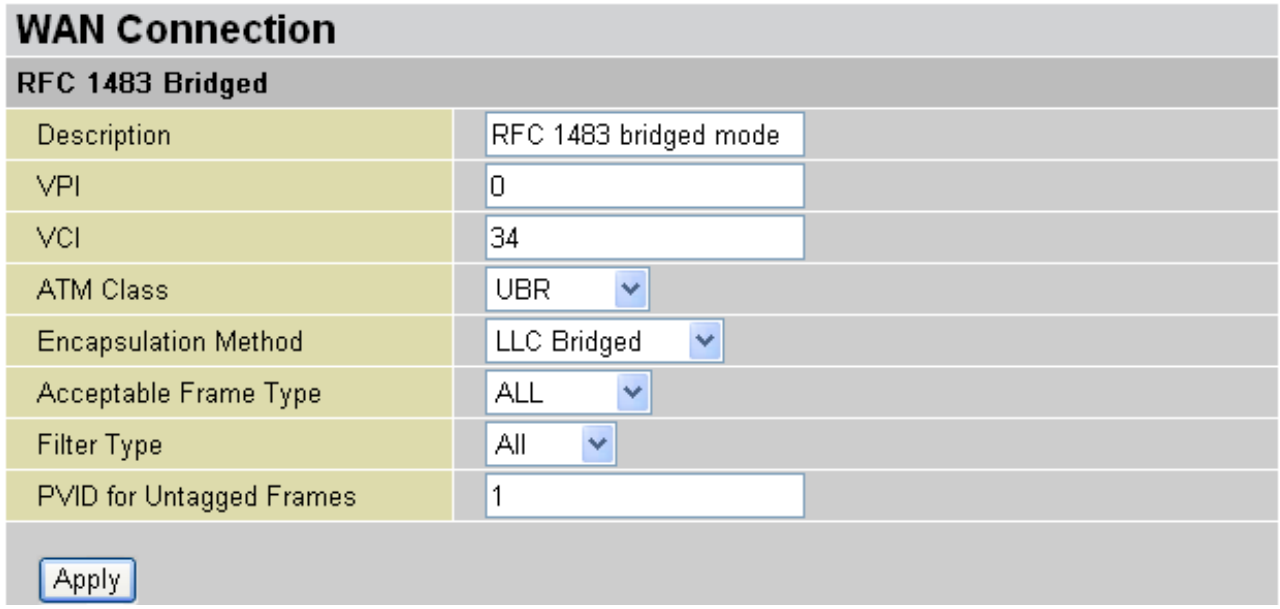
Click **Create** to setup up additional WAN interface for video applications. Total of 8 VLAN is support; therefore, only 8 WAN interfaces can be created in the table.



From the example, PVC 0/33 to 0/39 is assigned for video using 1483 Bridged mode. Check **RFC 1483 Bridged** and click **Next** to continue the setup.



Spaces next to VPI and VCI, type 0 and 33 in respectively. Select appropriate ATM Class, Encapsulation Method, Acceptable Frame Type, Filter Type and PVID for Untagged Frames.



VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

Acceptable Frame Type: Specify what kind of traffic can through this connection, all traffic or only VLAN tagged.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

PVID for Untagged Frames: PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID.

From the example, VPI and VCI only section need to be filled-in and just leave the rest as is. Repeat the same procedure by clicking **Create** → select **RFC1483 Bridged** → fill-in the rest of PVC 0/34 to 0/39.

WAN Connection

WAN Services Table

Name	Description	Creator	VPI	VCI		
wanlink	PPPoE WAN Link	QuickStart	0	40	Edit	Change
rfc1483-0	RFC 1483 bridged mode	WebAdmin	0	33	Edit	Delete
rfc1483-1	RFC 1483 bridged mode	WebAdmin	0	34	Edit	Delete
rfc1483-2	RFC 1483 bridged mode	WebAdmin	0	35	Edit	Delete
rfc1483-3	RFC 1483 bridged mode	WebAdmin	0	36	Edit	Delete
rfc1483-4	RFC 1483 bridged mode	WebAdmin	0	37	Edit	Delete
rfc1483-5	RFC 1483 bridged mode	WebAdmin	0	38	Edit	Delete
rfc1483-6	RFC 1483 bridged mode	WebAdmin	0	39	Edit	Delete

Step 3: Setup VLAN Service

Go to **Configuration → Advanced → VLAN Bridge**

DefaultVlan lists all member ports. It is necessary to group specific member ports for each VLAN.

From the example, two VLAN groups are requested: Data and Video.

To create another VLAN group for Video by clicking **Create VLAN.**

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit	

Create VLAN

Given a name and ID (PVID) to identify the Video group and the valid value range for PVID is 1 ~ 4094.

From the example:

VLAN untagged ports for Data/Internet: ethernet, wireless and wireless_wds.

VLAN untagged ports for Video: ethernet1, rfc-1483-0 ~ rfc-1483-6.

Click **Apply** to made change effective immediately.

Create VLAN

Parameters

VLAN Name	Video_VLAN	VLAN ID	2 (2~4094)
Tagged Member Port(s)	☐ ethernet ☐ wireless ☐ wireless_wds ☐ ethernet1 ☐ rfc1483-0 ☐ rfc1483-1 ☐ rfc1483-2 ☐ rfc1483-3 ☐ rfc1483-4 ☐ rfc1483-5 ☐ rfc1483-6		
Untagged Member Port(s)	☐ ethernet ☐ wireless ☐ wireless_wds ☑ ethernet1 ☑ rfc1483-0 ☑ rfc1483-1 ☑ rfc1483-2 ☑ rfc1483-3 ☑ rfc1483-4 ☑ rfc1483-5 ☑ rfc1483-6		

Apply Cancel Return

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,	Edit	
Video_VLAN	2	None	ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit	Delete

Create VLAN

Mapping the **VLAN Bridge** with **Bridge Interface** created in Step1, you will see the conformable relationship in these two screenshots.

Step 4: IGMP Snooping Enable

Go **Configuration → Advanced → IGMP**.

IGMP Snooping must be enabled in order to allow video stream forwarding correctly.

IGMP

Parameters

IGMP Forwarding	(•) Enable ( ) Disable
IGMP Snooping	(•) Enable ( ) Disable

Apply

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid them being lost after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.

Save Config to FLASH

Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to FLASH chips.

Apply

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting your service provider or Digicom support.

Problems starting up the router

Problem	*Corrective Action*
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with the WAN Interface

Problem	*Corrective Action*
Initialization of the PVC connection ("linesync") failed.	Ensure that the telephone cable is connected properly from the SHDSL port to the wall jack. The SHDSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router. If you still have problems, you may need to verify these settings with your ISP.

Problems with the LAN Interface

Problem	*Corrective Action*
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
	Verify that the IP address and the subnet mask are consistent between the router and the workstations.